U.S. Department of Transportation
Office of the Secretary of Transportation

ORDER

DOT 1630.2B

May 30, 2001

Subject: PERSONNEL SECURITY MANAGEMENT

1. PURPOSE. This order prescribes policies to ensure an effective and efficient personnel security program for the U.S. Department of Transportation (DOT) and to implement within DOT all applicable laws, Executive Orders (E.O.) and Governmentwide regulations pertaining to personnel security. It assigns responsibilities for the DOT program concerning employees being considered for initial or continued access to classified information.

2. CANCELLATIONS.

   a. DOT Order 1630.2A, DOT Personnel Security Program Handbook, dated May 27, 1988.

   b. DOT Order 1630.3, U.S. Department of Transportation Personnel Security Policies, dated November 17, 1972.

   c. DOT Security Bulletin SEC 96-02, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, dated August 6, 1996.

   d. DOT Security Bulletin SEC 96-04, Reciprocal Acceptance of Access Eligibility Determinations, dated June 13, 1997.

3. REFERENCES.

   a. E.O. 10450, Security Requirements for Government Employment, as amended, dated April 27, 1953.

   b. E.O. 12829, National Industrial Security Program, dated January 6, 1993.

   c. E.O. 12958, Classified National Security Information, as amended, dated April 17, 1995.

   d. E.O. 12968, Access to Classified Information, dated August 2, 1995.

   e. Title 5, Code of Federal Regulations (CFR), Parts 731, Personnel Suitability; 732, National Security Positions; and 736, Personnel Investigations.

   f. Investigative Standards for Background Investigations for Access to Classified Information, Security Policy Board (SPB) Issuance 1-97, approved by the President and dated March 24, 1997.

g. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, SPB Issuance 2-97, approved by the President and dated March 24, 1997.

h. Investigative Standards for Temporary Eligibility for Access, SPB Issuance 3-97, approved by the President and dated March 24, 1997.

i. Office of Management and Budget Circular No. A-130, Management of Federal Information Resources, revised February 8, 1996.

4. POLICY.

a. No person shall be employed or retained in employment by DOT unless a determination has been made on behalf of the Secretary of Transportation that such employment is clearly consistent with the interests of national security.

b. DOT shall grant a person eligibility for access to classified information only when facts and circumstances indicate that access to such information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

c. Within one year from the date of this order, or within 18 months of hiring, if hired after the date of this order, all personnel responsible for determining persons' eligibility for access to classified information shall have completed formal adjudicative training. The training curriculum shall meet the current training criteria used by the Department of Defense, the Department of Energy, or the Central Intelligence Agency when training adjudicative personnel and shall comply with any standards set by the SPB.

d. DOT shall grant no one access to classified information unless the required background investigation has been completed and favorably adjudicated, the person has a need for access to the classified information to perform his or her duties, and the person has signed an approved classified information nondisclosure agreement. In very exceptional circumstances, personnel security adjudicators may grant access to classified information to persons on whom the required investigations have not been completed, consistent with Governmentwide requirements for granting interim or temporary access.

e. DOT shall afford fair, impartial, and equitable treatment to all DOT employees and applicants through consistent application of personnel security standards, criteria, and procedures as specified in applicable laws, regulations, and orders. The department does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information, nor does the department use the denial of access to classified information as a substitute for appropriate adverse suitability determinations or disciplinary actions.

d. Employees shall:

(1) Be aware of the standards of conduct required for persons holding positions of trust, and recognize and avoid the kind of personal behavior that could result in rendering one ineligible for continued assignment in such a position. Employees are ultimately responsible for maintaining continued eligibility for these positions.

(2) As required by E.O. 12968, report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security. Employees should report such information to their servicing security organization.

(3) Familiarize themselves with security regulations that pertain to their assigned duties.

(4) Properly protect all classified information from unauthorized disclosure and report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to such information.

(5) Report all violations of security regulations to their servicing security organization.

6. DELEGATED PROGRAM AUTHORITY.

The Federal Aviation Administration (FAA), Federal Highway Administration (FHWA), and U.S. Coast Guard (USCG), are delegated authority to administer their own personnel security programs. These programs shall implement the policies of this order and DOT M 1630.2B, Personnel Security Management Manual. Subject to and following M-40 concurrence, the FAA, FHWA, and USCG may adopt procedures that implement DOT personnel security policies in ways different from those prescribed in the manual.

7. IMPLEMENTATION.

Except as permitted by paragraph 6, the policies and responsibilities set forth in this order and the procedural requirements contained in the Personnel Security Management Manual, DOT M 1630.2B, are for uniform application throughout DOT.

FOR THE SECRETARY OF TRANSPORTATION:

Melissa J. Allen

f. Nothing in this order shall limit or affect the responsibility and power of the Secretary, pursuant to any law or E.O., to deny or terminate access to classified information in the interest of the national security.

g. DOT shall provide all applicants, employees, and contractor personnel the opportunity to explain or refute any unfavorable information before the department uses the information as a basis for any adverse personnel, security, or similar action against them.

h. No person whom the Secretary has removed from employment for security reasons shall be employed by DOT without the Secretary's prior approval. This authority may not be redelegated.

i. Investigative and personnel security records may be disclosed only to the extent necessary under the requirements of this order and those DOT orders implementing the Privacy Act and the Freedom of Information Act.

5. RESPONSIBILITIES:

a. The Office of Assistant Secretary for Administration shall:

1. Direct and administer the DOT personnel security program.

2. Administer and implement DOT personnel security policies and ensure effective compliance with all laws, E.O. and regulations that govern the personnel security program.

3. Represent DOT with respect to other agencies and organizations both within and outside the Federal Government.

4. Periodically evaluate DOT's implementation of and adherence to personnel security policies and requirements.

5. Provide through the Director, Office of Security and Administrative Management, needed personnel security support services for the Office of the Secretary (OST) and for those DOT administrations and other organizations that have not been delegated their own personnel security operating authority.

6. As required, prepare consolidated personnel security program reports for and on behalf of the department.

b. Secretarial Officers and Heads of Operating Administrations shall:

(1) Implement policies promulgated by the Office of the Assistant Secretary for Administration and ensure that all provisions are effectively administered.

(2) Ensure that sufficient personnel and funding are provided to implement all DOT personnel security policies.

(3) Prepare and submit all required reports to OST.

(4) Inform the Office of Security and Administrative Management of any significant personnel security problems or issues.

(5) As warranted, promptly take all steps necessary to correct any personnel security program deficiencies.

c. Director, Office of Security and Administrative Management (M-40) shall:

(1) Provide guidance and direction throughout DOT on all personnel security matters.

(2) Provide personnel security support services for OST and all DOT organizations to which the Assistant Secretary for Administration has not delegated specific personnel security operating authority.

(3) Evaluate all DOT personnel security activities and, as appropriate, either make or recommend needed changes in policies and procedures.

(4) Provide liaison with other Government agencies as needed on personnel security matters.

(5) Authorize exceptions to DOT personnel security policies and procedures when doing so meets an urgent management need, is consistent with the interests of national security, does not infringe on the rights of any employee or applicant, and does not conflict with authority reserved by either the Secretary or the Assistant Secretary for Administration.

PERSONNEL SECURITY MANAGEMENT MANUAL

Office of Security and Administrative Management
Office of the Assistant Secretary for Administration
Office of the Secretary

PERSONNEL SECURITY MANAGEMENT MANUAL

TABLE OF CONTENTS

Chapter 1 - General Information

Section 1 - Purpose..... I-1
Section 2 - Delegated Program Authority..... I-1
Section 3 - References to Days..... I-2
Section 4 - Definitions..... I-2

Chapter 2 - Personnel Security Operations and Specific Responsibilities

Section 1 - Standards of Operation and Specific Responsibilities..... II-1
Section 2 - Safeguarding Employees' and Applicants' Rights and Privacy..... II-4
Section 3 - Release of Personnel Security Records..... II-5

Chapter 3 - Suitability and Personnel Security Standards

Section 1 - Relationship between Suitability and Security..... III-1
Section 2 - Personnel Security Standard and Criteria..... III-2

Chapter 4 - Position Sensitivity and Risk Level Designation

Section 1 - General Requirements and Definitions.....IV-1
Section 2 - Specific Requirements and Process for Designation..... IV-3

Chapter 5 - Personnel Security Investigation Requirements

Section 1 - Types and Scope of Background Investigations..... V-1
Section 2 - Basic Investigative Requirements..... V-3
Section 3 - Exceptions to Investigative Requirements..... V-6
Section 4 - Waiver of Pre-placement Investigative Requirements for Special-Sensitive and Critical-Sensitive Positions..... V-7

Section 5 - Financial and Foreign Travel Disclosure Requirements..... V-9
Section 6 - Investigative Requirements for Non-Federal Personnel..... V-9
Section 7 - Forms..... V-10

Chapter 6 - Reciprocity and Standards for Using Previous Investigations

Section 1 - General..... VI-1
Section 2 - Obtaining and Reviewing Previous Investigations..... VI-2

Chapter 7 - Role of Security in Suitability Adjudication

Chapter 8 - Security Adjudication

Chapter 9 - Access to Classified Information

Section 1 - General..... IX-1
Section 2 - Limitations and Restrictions on Access to Classification Information..... IX-2
Section 3 - Request Procedures..... IX-3
Section 4 - Interim Clearances..... IX-4
Section 5 - Final Clearances..... IX-6
Section 6 - Temporary Clearances..... IX-6
Section 7 - Clearance Granting Procedures and Documentation..... IX-7
Section 8 - Terminating Access Authorizations..... IX-8
Section 9 - Special Access Authorizations..... IX-9
Section 10-Security Clearances for National Defense Executive Reserve (NDER) Personnel and Federal Port Controllers..... IX-11
Section 11-Security Clearances and Authorizations for Non-United States Citizens..... IX-12

Chapter 10 - Adverse Security Actions

Section 1- General..... X-1
Section 2 - Security Clearance Denial, Suspension, and/or Revocation..... X-1
Section 3 - Suspension and Removal Under Title 5 U.S.C. 7532..... X-4
Section 4 - Employment of Individuals Previously Separated for Security Reasons..... X-6

Chapter 11 - Foreign Assignments and Travel

Appendix 1 - Security Adjudication Guidelines

Appendix 2 - Investigating Contractor Employees

Appendix 3 - National Industrial Security Program

Appendix 4 - Investigating Child Care Services Workers

Appendix 5 - Position Risk Level Designation Process

Chapter 1

GENERAL INFORMATION

Section 1 - Purpose

1-1. The purpose of this manual is to implement the policies of Order 1630.2B, Personnel Security Management, and to establish a uniform personnel security program for the Department of Transportation (DOT). This program is designed to protect classified information, ensure cost effectiveness, and provide fair and equitable treatment to all DOT employees and applicants considered for initial or continued access to classified information, consistent with the interests of national security. It also includes the initiation and processing of required background investigations on all Federal employees and certain contractor employees.

1-2. This manual sets forth the standards, criteria, and guidelines for personnel security determinations; describes the types and scopes of personnel security investigations; specifies investigative requirements; and states the procedures for adverse security actions in regard to individuals' access to classified national security information.

1-3. This manual addresses the relationship between security and suitability determinations with respect to the hiring or retention of persons for DOT employment.

1-4. This manual contains requirements and procedures for conducting investigations on contractor employees and child care center workers. It also contains basic procedures for processing contractor employees for access to classified information under the provisions of the National Industrial Security Program (NISP).

1-5. For purposes of this manual, the term DOT organization is defined as including all Secretarial organizations and Operating Administrations, the Bureau of Transportation Statistics, and the Transportation Administrative Service Center.

Section 2 – Delegated Program Authority

1-6. The Federal Aviation Administration (FAA), Federal Highway Administration (FHWA), and United States Coast Guard (USCG) are delegated authority to administer their own personnel security programs. These programs shall implement the policies of Order 1630.2B and this manual. Subject to and following Office of Security and Administrative Management (M-40) concurrence, the FAA, FHWA, and USCG may adopt procedures that implement DOT personnel security policies in ways different from those prescribed in this manual.

Section 3 – References to Days

1-7. In this manual, and unless otherwise stated, all references to days refer to calendar days.

Section 4 - Definitions

Access. In general, the ability to enter and/or pass through an area or a facility; or the ability or authority to obtain information or monetary or material resources. In relation to classified information, the ability, authority, and/or opportunity to obtain knowledge of such information.

Access authorization. Certification that a person is currently authorized to have access to classified information at specific levels.

Appointing/approving official. The individual delegated the authority to effect appointments, reassignments, promotions, separations, or similar personnel actions regarding DOT employees or applicants.

Background investigation. Any personnel investigation conducted to meet personnel security program requirements.

Background Investigation (BI). An investigation consisting of a National Agency Check (NAC), credit search, personal interviews of subject and sources, written inquiries, and record searches covering specific areas of a person's background during the most recent 5 years, and additional record searches during the most recent 7 years.

Classified information. Official information or material that requires protection in the interest of national security and is classified for such purpose by appropriate classification authority in accordance with the provisions of Executive Order (E.O.) 12958, Classified National Security Information, or any successor authority.

Cohabitant. An individual with whom the subject lives, other than a spouse, child, or other relative (mother, father, brother, sister, in-laws, etc.), with whom a bond of affection, influence, obligation, or a spouse-like relationship exists.

Contract. As defined in Federal Acquisition Regulation 2.101, a mutually binding legal relationship obligating the seller to furnish supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include, but are not limited to, awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by

written acceptance or performance; and bilateral contract modifications. This includes reimbursable agreements and interagency agreements.

Contracting officer. As defined in Federal Acquisition Regulation 2.101, a person with the authority to enter into, administer, and/or terminate contacts and make related determinations and findings. The term includes certain authorized representatives of the contracting officer acting within the limits of their authority as delegated by the contracting officer.

Contractor employee. A person hired by a contractor as an employee or subcontractor to perform tasks under a DOT contract. This term includes any consultant to DOT who is not actually a Federal employee.

Defense Clearance and Investigations Index (DCII). An automated index of all investigations conducted by the Department of Defense (DOD) on military personnel, DOD civilian employees, and applicants.

DOT employee. Any person employed directly by DOT, including a member of the USCG.

Foreign national. An individual who is not a citizen of the United States.

Immigrant alien. An individual who is lawfully admitted to the United States under an immigration visa for permanent residence.

Interim access authorization. An authorization for access to classified information granted pending completion of the required investigation.

Limited Background Investigation (LBI). An investigation consisting of a NAC, credit search, personal interviews of subject and sources, written inquiries of selected sources covering specific areas of a person's background during the most recent three years, and record searches for a total of five 5 years' coverage.

Limited Access Authorization. A certification that a person is authorized to have access only to certain specified classified information that has been carefully screened by security officials for its release to that person.

Local Agency Check (LAC). A check of records at a state or local law enforcement agency.

Minimum Background Investigation (MBI). An investigation consisting of a National Agency Check and Inquiries (NACI), a credit search, and telephone inquiries to follow up on written inquiries not returned.

National Agency Check (NAC). An investigation consisting of searches of the following files: Security/Suitability Investigations Index (SII), DCII, the Federal Bureau of Investigation's (FBI) Identification Division, and the FBI's Records Management Division.

National Agency Check and Inquiries (NACI). An investigation consisting of a NAC, written inquiries, and record searches covering specific areas of a person's background during the most recent five years.

National security. The protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs, from overt and covert attack, against or from espionage, sabotage, and subversion, and any and all illegal acts designed to weaken or destroy the United States.

National security position. A position involving Government activities concerned with the protection of the national security.

Need-to-Know. A determination made by an authorized holder of classified information that a prospective recipient requires access to, knowledge of, or possession of specific classified information to perform or assist in a lawful and authorized U.S. Government function or program.

Periodic Reinvestigation (PRI). An investigation updating a previous investigation and consisting of a NAC, credit search, personal interview of the subject, and selected record searches.

Periodic Reinvestigation for SSBI (SSBI-PR). An investigation updating a Single Scope Background Investigation (SSBI) and consisting of personal interviews of the subject and sources, a NAC, credit search, and written inquiries and record searches covering specific areas of a person's background during the most recent five years.

Personnel security. The standards and procedures utilized to determine and document that the employment or retention in employment of an individual will promote the efficiency of the service and is clearly consistent with the interests of the national security.

Personnel security adjudicator. An individual in the servicing security organization who conducts security adjudication.

Personnel security officer. A specifically appointed individual within a servicing security organization who is primarily responsible for management and operation of the personnel security program.

Position risk level. The designation of a position based on its public trust responsibilities and attributes as they relate to the efficiency of the service.

Position sensitivity. The designation of a national security position based on its relative importance to the national security.

Proprietary Information. Confidential commercial or financial information.

Public trust position. A position that has the potential for action or inaction by an incumbent to affect the integrity, efficiency, or effectiveness of assigned Government activities.

Reimbursable Suitability Investigation (RSI). An investigation conducted by the Office of Personnel Management (OPM) to resolve a suitability issue raised in a previous investigation.

Resources. Material and monetary items of value, including facilities, equipment (including, but not limited to, computers, facsimile machines, photocopiers, printers, and furniture), information databases (both hardware and software), and records in whatever form they exist.

Scope. The time period to be covered and the sources of information to be contacted during the prescribed course of a personnel security investigation.

Security adjudication. The determination as to whether the employment or continued employment of an individual, and the person's access to classified information, if necessary, can reasonably be expected to be clearly consistent with the interests of national security.

Security/Suitability Investigations Index (SII). OPM's index of investigations conducted by OPM and by other agencies as reported to OPM.

Servicing security organization. The organizational element that is responsible for providing security services to a particular DOT administration or organization.

Single Scope Background Investigation (SSBI). An investigation consisting of a NAC, birth records search, credit search, personal interviews of subject and sources, written inquiries, and record searches covering specific areas of a person's background during the most recent 10 years.

Suitability. Identifiable character traits and past conduct which are sufficient to determine whether or not a given individual is likely to carry out the duties of a Federal job with appropriate efficiency and effectiveness.

Suitability adjudication. The process of determining a person's suitability for Federal employment in a particular position.

Temporary clearance. An authorization for access to classified information granted for a limited period of time.

Unauthorized Disclosure. A communication or physical transfer of classified information to a recipient unauthorized to receive it in the given circumstances.

Upgrade Investigation (UGI). An investigation consisting of a NAC, credit search, personal interviews of the subject and selected sources, and record searches covering specific areas of a person's background since the last investigation. This investigation is for movement upward in sensitivity/risk level from between 13 to 60 months of the previous investigation's closing date.

Update Investigation (UDI). An investigation consisting of the same type of coverage as a previous investigation, conducted from between 13 and 60 months of that investigation.

Chapter 2

PERSONNEL SECURITY OPERATIONS AND RESPONSIBILITIES

Section 1 – Standards of Operation and Specific Responsibilities

2-1. Standards. DOT personnel security operations shall meet the following standards:

a. The operations shall be conducted at organizational levels where they are closely controlled to ensure that they comply with DOT requirements and are managed in an efficient and effective manner.

b. In servicing security organizations, only professionally qualified personnel security officers shall direct personnel security operations. Security managers may delegate responsibility for security adjudication, but may do so only to specialists who are fully trained to evaluate reports and results of personnel investigations and who have successfully completed an approved personnel security adjudication course.

2-2. Operational responsibilities. Personnel security officers and specialists have primary responsibility for personnel security operations. However, human resources and employing office officials shall assist them by performing certain personnel security operational duties.

a. The servicing security organization shall:

(1) Work with employing offices and human resources organizations as needed to ensure that position sensitivity and risk level designations are accurate for all positions within its area of responsibility.

(2) Review investigative forms for completeness, confirm the necessity for investigations, and initiate personnel security investigations as required.

(3) Check national investigations indices for prior investigations concerning applicants and employees.

(4) Process requests for waiver of pre-placement investigative requirements. Conduct local agency and other checks as necessary.

(5) Receive from OPM or other sources results of all investigations on applicants and employees. Review investigative reports to determine the adequacy of the investigations and to identify security or suitability issues.

(6) Conduct or arrange for any additional investigation necessary to resolve security or suitability issues.

(7) Provide due process to applicants and employees when required by Section 2 of this chapter.

(8) Make security determinations on all cases involving sensitive positions and grant or deny access to classified information; i.e., security clearances. Advise human resources organizations of these determinations.

(9) When requested, advise and assist human resources organizations and/or employing offices in adjudicating suitability on applicants or employees.

(10) Prepare and conduct, or ensure that employing offices conduct, security briefings for employees as needed.

(11) Provide guidance to human resources organizations and employing offices on personnel security policies and operating procedures.

(12) Periodically evaluate its personnel security program to ensure that it is operating effectively and efficiently.

(13) Process visit clearance requests and certify security clearances as necessary.

(14) Advise employing offices and human resources organizations of all changes in costs of background investigations.

b. The employing office shall:

(1) Recommend position sensitivity and risk level designations on positions under its jurisdiction and coordinate with the servicing security organization regarding final designations.

(2) Ensure that all Optional Form 8's (OF-8), Position Description, or equivalent, either electronic or hard-copy, show the approved sensitivity or risk level designation, as well as any requirement for access to classified information.

(3) When appropriate, ensure that vacancy announcements state that appointment is subject to a favorably adjudicated personnel security investigation enabling the granting of a security clearance.

(4) Ensure that before placing, or making any commitment to place, a person in a special-sensitive, critical-sensitive, or noncritical-sensitive position, the servicing security organization has determined that the pre-placement investigative requirement has been met or that an appropriate waiver has been granted.

(5) Request waivers from or through the servicing security organization of pre-placement investigative requirements when emergency conditions exist that preclude meeting them.

(6) Budget for the costs of conducting personnel investigations, or coordinate with the servicing security organization to ensure budgeting for these costs.

(7) Obtain or assist human resources organizations in obtaining personnel security questionnaires, fingerprints, and other forms as required for personnel security processing. Ensure that paperwork is properly completed and submitted in time to initiate investigations as required by Chapter 5.

(8) Conduct or arrange for security briefings for new employees and employees with newly granted security clearances. Periodically conduct or arrange for additional briefings to maintain a high level of security awareness.

(9) Advise the servicing security organization of any questionable conduct or activity by an employee that would raise a security or suitability issue.

(10) Maintain records of the risk and sensitivity levels of its organization's positions.

(11) Maintain records of the security clearances held by its organization's employees. Maintain records as required by those directives that implement the Privacy Act.

c. Human resources organizations shall:

(1) Coordinate with the servicing security organization on each new or revised position description as needed to ensure that the original OF-8 or equivalent shows the approved risk or sensitivity level.

(2) Ensure that all vacancy announcements contain appropriate information about any investigative or personnel security clearance requirements that are a condition of employment in the position.

(3) Obtain or participate with employing offices in obtaining personnel security questionnaires, fingerprints, and other forms as required for personnel security processing. Ensure that paperwork is properly completed and submitted in time to initiate investigations as required by Chapter 5.

(4) When an applicant is a current or former Federal employee, obtain available Official Personnel Folder (OPF) data about previous investigation(s). Provide this information to the servicing security organization when the person is applying for other than a low-risk position, and advise the security organization whenever the OPF contains no conclusive proof of a prior investigation.

(5) Coordinate with the security organization regarding any information about an applicant that would raise a security or suitability issue. This includes information disclosed on an employment application or personnel security questionnaire, or from pre-placement inquiries, prior employers, the OPF, or any other sources.

(6) Refer to the security organization any information about an employee that would raise a security or suitability issue.

(7) Obtain approval from the servicing security organization before placing any person in a special-sensitive, critical-sensitive, or noncritical-sensitive position; and, before placing any person in a high risk or moderate risk position, ensure that the requirements of paragraphs 5-12 and 5-13 have been met.

(8) Maintain accurate and current records of the sensitivity or risk-level designation for each position.

Section 2 - Safeguarding Employees' and Applicants' Rights and Privacy

2-3. Applicants and employees shall be afforded an opportunity to explain, refute, or deny any unfavorable information obtained as the result of a personnel security investigation before DOT may take any unfavorable action based on that information, including denial of a benefit to which an individual would otherwise be entitled. The individual has the right to make an oral or written reply. This practice, commonly known as due process, prevents errors which might otherwise result from mistakes in identity or erroneous information and provides the applicant or employee the opportunity to present mitigating information that may be unknown to the adjudicating officials. The applicant or employee must be provided any appropriate Privacy Act advice. Any record of the unfavorable information, to include the applicant's or employee's response to it, may be furnished only to those individuals who, in their official capacity, have a need to know such information.

2-4. Investigative information obtained under a pledge of confidence shall be controlled in accordance with the commitment the investigating agency made to the source of that information.

2-5. Medical information of a sensitive, personal nature that is obtained in conjunction with an investigation shall be carefully controlled to ensure that it is not disclosed to individuals who do not need it for official purposes. It also shall not be used to make a security or suitability determination until it has been properly interpreted by a medical official trained in analysis of the specific type of medical information concerned. If the medical official concludes that it might be harmful to an applicant or employee to see any of the medical information, access to that information shall be denied to the individual except through a medical official chosen by him or her.

2-6. The servicing security organization shall ensure that before releasing investigative information to anyone outside the security organization, the persons to whom the information is being disclosed have a need to know it in an official capacity and in order to carry out a responsibility prescribed by this directive. All persons receiving investigative information shall similarly ensure that it is disclosed only to persons who have a need to know it in an official capacity.

2-7. All Personnel Security Files (PSF), reports of personnel investigations, personal history statements, records of response to derogatory information, computerized personnel security data, and other personnel security records and documents shall be regarded as Privacy Act information. During handling, transmission, release, and storage, they shall be carefully protected in accordance with all DOT procedures regarding this type of information. The information shall also be protected from disclosure, to the extent allowed by law, when responding to Freedom of Information Act (FOIA) requests for these types of records.

Section 3 - Release of Personnel Security Records

2-8. Upon request, a servicing security organization shall provide an employee the opportunity to review his or her PSF. The employee may also, in writing, authorize a representative to review it. The security organization shall do the following when complying with a request for a PSF review:

a. Review the file before letting the employee or representative review it, or before sending it to a field facility for review.

b. Remove any report of investigation completed by another agency, such as OPM, the Defense Security Service (DSS), or the FBI. If such a report is removed, inform the employee or representative in writing that the original of the PSF contains a report completed by (name of agency), that neither DOT nor an

individual DOT organization is authorized to release it directly to the employee or representative, and that he or she should contact the investigating agency directly in order to request a copy.

c. Remove from the file any other information, such as identification of a confidential source or that concerning an ongoing investigation, that is exempt from release under the Privacy Act.

d. If the employee works at a field location distant from the security organization, send only a certified true copy of the PSF to the employee's facility, retaining the original in the security organization. Enclose the copy in an envelope addressed to the employee and marked, "TO BE OPENED BY ADDRESSEE ONLY."

e. When the review takes place at the security organization, permit the employee or representative to review the PSF or make copies of documents in it only under the direct observation of an security employee. Provide the employee or representative a reasonable amount of time to review the file and ensure that he or she does not withdraw any documents or pages from it.

f. Any request for access shall be evaluated under both FOIA and the Privacy Act, regardless of which the requester cites, and access shall be granted under whichever statute, in specific circumstances, provides greater access.

2-9. In responding to requests under the Privacy Act for disclosure of information in PSF's and/or reports of investigation, DOT personnel shall follow all DOT and all of their administration's or organization's policies on implementing the Privacy Act. However, no report of investigation completed by another Federal agency shall be released in response to a Privacy Act request without the consent of that agency. Neither DOT nor an individual DOT organization is authorized to release such a report outright, as that is the prerogative of the agency that prepared it. If an individual asks for a copy of his or her PSF, and the PSF contains another agency's report of investigation, the person shall be told that the PSF contains the report, which agency prepared it, and that DOT is not authorized to release it without the other agency's consent. In the case of an OPM report of investigation, and because OPM has requested this procedure, the individual should be told to contact OPM directly to ask for a copy.

2-10. Without the concurrence of the servicing security organization, no collective bargaining agreement or agreement with an individual shall be entered into requiring DOT or any DOT organization to release any personnel security record. Under no circumstances shall any agreement be entered into requiring DOT to release a report of investigation completed by another Federal agency.

CHAPTER 3

SUITABILITY AND PERSONNEL SECURITY STANDARDS

Section 1 - Relationship Between Suitability and Security

3-1. Suitability means fitness or eligibility for employment and refers to identifiable character traits and past conduct that are sufficient to determine whether a given individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate efficiency and effectiveness. Suitability is distinguishable from a person's ability to fulfill the qualifications requirements of a job, as measured by experience, education, knowledge, skills, and abilities. The focus of a suitability adjudication is on whether the employment or continued employment of an individual can reasonably be expected to promote the efficiency of the Federal service. 5 CFR Part 731, Suitability, contains potentially disqualifying suitability factors for competitive service employees and states the circumstances under which persons may be disqualified for employment for suitability reasons.

3-2. Security relates to requirements for an individual occupying a specific position to have access to classified information. A security determination focuses on the question of whether or not access to such information is clearly consistent with the interests of the national security. Section 2 of this chapter contains the standard and criteria specified in E.O. 10450 and E.O. 12968, which shall be used in making a security determination.

3-3. In processing applicants for employment, a security determination under E.O. 10450 and/or E.O. 12968 will usually be made subsequent to a favorable suitability adjudication. Therefore, a human resources organization may favorably adjudicate a background investigation or information the applicant has provided and find the person suitable for employment in a specific sensitive position; but the servicing security organization would then separately determine whether or not the person should have access to classified information. In the case of an employee, however, neither a suitability adjudication nor a security determination is contingent upon the other. For example, a security determination may result in reassignment or removal from a position under the provisions of Chapter 10, even if the servicing human resources organization has made no suitability determination. Also under those provisions, a security determination that an employee may not be granted a security clearance would prevent promotion or reassignment to a sensitive position.

3-4. Certain employees may not be subject to suitability determination by their human resources organization, depending on such factors as their status and length of employment. An example would be competitive service employees who have been employed for more than 1 year and who are not subject to suitability action under 5 CFR Part 731. They are, however, subject to disciplinary and removal actions when an investigation develops information warranting such action. Whenever a personnel security investigation develops unfavorable information that could potentially be the basis for a disciplinary or removal action, the servicing security organization shall provide human resources and other

management officials, as appropriate and on a need-to-know basis, all investigative reports and other information necessary to enable these officials to take appropriate action.

Section 2 -- Personnel Security Standard and Criteria

3-5. Security Standard. The granting of access to classified information to any person shall be clearly consistent with the interests of the national security. In making this determination, the adjudicator assesses past and present conduct and considers whether or not the granting of such access conforms to this standard. Conduct relating to any of the criteria listed below is grounds for denying access to classified information if the conduct indicates that the person would pose a risk for damage to the national security. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Servicing security organizations shall grant this eligibility only when doing so is clearly consistent with the national security interests of the United States and any doubt shall be resolved in favor of the national security.

3-6. Criteria. E.O. 12968 states that eligibility for access to classified information shall be granted only to persons whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment; freedom from conflicting allegiances and potential for coercion; and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. E.O. 10450 enumerates the following criteria which shall be considered in making security determinations:

a. Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

b. Any deliberate misrepresentation, falsification, or omission of material facts.

c. Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion.

d. Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.

e. Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause the person to act contrary to the best interests of the national security.

f. Commission of any act of sabotage, espionage, treason, terrorism, sedition, or attempts, threats, or preparation thereof, or conspiring with, or aiding or abetting another to commit or attempt to commit any act of sabotage, espionage, treason, terrorism, or sedition.

g. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation whose interest may be inimical to the interest of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

h. Advocacy of use of force or violence to overthrow the Government of the United States, or of the alteration of the form of Government of the United States by unconstitutional means.

i. Knowing membership with specific intent of furthering the aims of or adherence to and active participation in any foreign or domestic organization, association, movement, group, or combination of persons which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state, or which seeks to overthrow the Government of the United States or any state or subdivision thereof by unlawful means.

j. Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

k. Performing or attempting to perform duties or otherwise acting so as to serve the interest of another Government in preference to the interests of the United States.

l. Refusal by the individual upon the ground of constitutional privilege against self-incrimination to testify before a congressional committee regarding charges of alleged disloyalty or other misconduct.

3-7. Restrictions. E.O. 12968 specifies the following restrictions in applying the security standard and criteria:

a. In granting access to classified information there shall be no discrimination on the basis of race, color, religion, sex, national origin, disability, or sexual orientation.

b. In determining eligibility for access, an agency may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. However, no inference concerning the security standard and criteria may be raised solely on the basis of a person's sexual orientation.

c. No negative inference concerning the security standard and criteria may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standard and criteria are satisfied, and mental health may be considered when it directly relates to the standard and criteria.

3-8. Coordinating information. Human resource management officials and all DOT supervisors shall furnish to their servicing security organization any information they receive concerning employees or applicants under their jurisdiction that may affect their suitability for employment or their holding of a security clearance because of the standards and criteria stated in this section.

Chapter 4

POSITION SENSITIVITY AND RISK LEVEL DESIGNATION

Section 1 - General requirements and definitions

4-1. All DOT positions must be designated as to their level of risk in terms of suitability and access to Automated Information Systems (AIS), and level of sensitivity in terms of national security.

a. Sensitivity Designation. Every position having national security duties must be designated at a national security sensitivity level necessary to ensure appropriate screening under E.O. 10450. Sensitivity designation is based on an assessment of the degree of damage that an individual occupying a particular position could cause to the national security.

b. Risk Level Designation. Every position not receiving a designation as a national security position shall be designated at a position risk level commensurate with the public trust responsibilities and attributes of the position as they relate to the efficiency of the service. The suitability risk levels are ranked according to the degree of adverse impact on the efficiency of the service that an unsuitable person could cause. Every position where the incumbent has access to or the responsibility for AIS facilities, systems, or activities must be designated at a risk level commensurate with the responsibilities and other attributes of the position based on the extent to which an incumbent could cause damage to an AIS or realize significant personal gain.

4-2. The servicing security organization, working with human resources organizations and employing offices, has overall responsibility for ensuring the correct risk and sensitivity level designation of every position within its jurisdiction. All new position descriptions, or groups of position descriptions, should be coordinated with the security organization before sensitivity or risk levels are designated, and the security organization shall approve any changes in a position's sensitivity or risk level designation. Designations may be by class, group, or categories of positions, when appropriate, or may be by an individual position when circumstances warrant.

4-3. There are three position risk levels, as follows:

a. Low Risk. These are positions that have potential for impact involving duties of limited relation to the agency mission with program responsibilities which affect the efficiency of the service. This level includes positions that have limited impact on AIS.

b. Moderate Risk. These are public trust positions that have the potential for moderate to serious impact involving duties of considerable importance to the agency or program mission with significant program responsibilities and delivery of customer services to the public. This level includes positions which have significant program responsibilities that affect large AIS.

c. High Risk. These are public trust positions which have the potential for exceptionally serious impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority. This level includes positions that have major program responsibilities affecting AIS.

4-4. There are three sensitivity levels for designating positions with regard to national security:

a. Noncritical-sensitive (NCS). These are positions with potential for causing serious damage to the national security.

b. Critical-sensitive (CS). These are positions with the potential for causing exceptionally grave damage to the national security.

c. Special-sensitive (SS). These are positions that an agency determines to be at a level higher than critical-sensitive because of special requirements other than authority under E.O. 10450. This category includes all positions requiring access to SCI.

4-5. Servicing security organizations shall use the risk level designation process outlined in Section 2 of this chapter and Appendix 5, Position Risk Level Designation Process, or a similar process issued or approved by M-40, to ensure that DOT designates positions uniformly and consistently. This process includes the criteria for designating risk levels based on AIS duties and responsibilities. Servicing security organizations shall use the national security criteria for determining sensitivity levels in conjunction with the risk level designation process to ensure proper designation of national security positions.

a. All positions requiring access to classified information are sensitive positions and shall be designated at one of the three sensitivity levels. Section 2 specifies the minimum sensitivity level for each level of access.

b. In many cases, particularly at the low-risk level, position risk is relatively clear and it may not be necessary to apply all of the specific designating procedures in Section 2 or in a more specific process. Similarly, essentially identical

positions may require only occasional case-by-case analysis. Even when risk levels may appear to be obvious, specific procedures should be applied on at least a random basis to ensure proper designations.

c. National security positions, particularly those requiring Top Secret or SCI access, can frequently be designated at the appropriate sensitivity level without applying more detailed procedures. However, if the duties and responsibilities of a national security position warrant designation as a high-risk position, the position must be designated at least critical-sensitive, even if the level of access required is no higher than Secret.

4-6. Position risk and sensitivity level designation shall be documented on DOT Form 1630.2, Determination of Position Sensitivity, contained in Appendix 5, or a comparable form. The human resources organization shall maintain this form unless the servicing security organization agrees to do so. Even if the human resources organization keeps it, the security organization shall maintain copies of the forms for sensitive positions. The form may also be maintained electronically in lieu of retaining hard copies.

4-7. The following coding of position risk and sensitivity levels is required for Governmentwide use on appropriate personnel documents such as the SF 50, Notification of Personnel Action, and SF-52, Request for Personnel Action. It shall be used to record a position's level in any DOT automated system containing that information.

RISK/SENSITIVITY LEVEL	CODING
High risk	6
Moderate risk	5
Special-sensitive	4
Critical-sensitive	3
Noncritical-sensitive	2
Low risk	1

Section 2 – Specific requirements and process for designation

4-8. Sensitivity level designation:

a. As stated in Section 1 of this chapter, all positions requiring access to classified information, and therefore having national security duties, are sensitive positions and shall be designated as either noncritical-sensitive, critical-sensitive, or special-sensitive. Listed below are the minimum sensitivity levels for positions requiring access to specific levels of classified information:

(1) Positions requiring access to Confidential or Secret information shall be designated at least noncritical-sensitive.

(2) Positions requiring access to Top Secret information shall be designated at least critical-sensitive.

(3) Positions requiring access to SCI shall be designated special-sensitive.

b. When it is apparent that the risk level criteria described below would not affect a sensitivity level determination that is based on access to classified information, the designation process need not consist of anything other than appropriately documenting the designation. For example, if a position requires access to SCI, it will automatically be special-sensitive regardless of other risk factors involved.

4-9. The risk level designation process consists of designating each position for its degree of risk to its program, based on the descriptions in Section 1 above, and making any final adjustments necessary because of unique factors specific to certain positions or to ensure organizational uniformity of operations. Appendix 5 describes one process that DOT organizations may use in making initial risk level determinations. M-40 may also issue more specific guidelines and procedures for use in the designation process.

4-10. Some positions, by the very nature of the duties and responsibilities of the program or the positions, require designation at certain levels of risk.

a. Uniqueness. Factors that are unique, that are not fully accounted for in the above procedures, and that can cause final adjustments include:

(1) Special investigative or criminal justice duties.

(2) Control of an automated monetary system (key access entry).

(3) Few-of-a-kind positions with special duties, such as special assistant to the Administrator.

(4) Support positions with no responsibilities for preparation or implementation of public trust program policies and plans, but involving regular contact with and ongoing knowledge of all or most of such material; e.g., budget analyst.

(5) Any other factors believed relevant, provided they are documented.

b. Uniformity. Clearly indicated needs for uniformity in position designation

because of authority level or program placement level that may serve as a basis for making adjustments include:

(1) The need for managers of major agency programs or divisions at the same level of authority to be placed at the same risk level.

(2) The need for all positions within a particular program to be at a risk level paralleling the program's placement level. This would occur in those cases where the placement level is determined to be so overriding as to negate any specific risk considerations associated with individual positions within the program.

c. Final adjustment.

(1) Any decisions on adjustment should be made only after careful analysis of positions in terms of any uniqueness or uniformity factors that may apply. The persons designating positions shall document all adjustment factors used for a given position.

(2) In order to ensure uniformity and consistency in risk level designations, security organizations should assist DOT organizations they service as necessary in reviewing position descriptions for positions common in more than one major organization; for example, secretary, accountant, safety inspector, etc.

4-11. AIS positions :

a. Risk level criteria for positions involving access to AIS are an integral part of risk and sensitivity level designation. In addition to any public trust or national security criteria that may apply, the following criteria shall apply to any position with AIS duties and responsibilities:

(1) High risk. Includes any position at the highest level of risk to an AIS. This is to include positions in which the incumbent is responsible for the planning, direction, and implementation of an AIS security program; has a major responsibility for the direction, planning, and design of an AIS, including the hardware and software; or can access a system during its operation or maintenance in such a way that there is relatively high risk for causing grave damage or realizing a significant personal gain. Such positions may involve:

(a) Responsibility for the development and administration of DOT AIS security programs, including direction and control of risk analyses and/or threat assessments.

(b) Significant involvement in life-critical or mission-critical systems.

(c) Responsibility for the preparation or approval of data for input into an AIS that does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

(d) Relatively high-risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from an AIS of (1) dollar amounts of $10 million per year or greater or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority to ensure the integrity of the system.

(e) Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

(f) Other positions that involve relatively high risk for effecting grave damage or realizing significant personal gain.

(2) Moderate risk. Includes positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of an AIS, and whose work is technically reviewed by a higher authority at the high-risk level to ensure the system's integrity. Such positions may involve:

(a) Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority at the high-risk level to ensure the integrity of the system. This level includes, but is not limited to:

(1) Access to and/or processing of proprietary data, information protected by the Privacy Act, and Government-developed privileged information involving the award of contracts. This criterion applies when the

access is to a major DOT AIS and not just to information contained in a personal computer or local area network. The nature, extent, and volume of the information shall be considered in applying this criterion.

(2) Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less then $10 million per year.

(b) Other positions that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in high-risk positions.

(3) Low risk. Includes all AIS positions not falling into one of the above risk levels.

b. As positions with AIS duties and responsibilities may also involve determinations under the criteria and procedures elsewhere in this section, or issued separately, the higher of the levels determined applying both sets of criteria or procedures shall be used as the final risk level. If the position is sensitive because of national security responsibilities, a determination of high risk under the AIS criteria shall result in a designation of at least critical-sensitive. Adjustments due to AIS criteria shall be documented.

c. Positions in the following job series shall be considered as AIS positions: 332, Computer Operator; 334, Computer Specialist; 335, Computer Clerk or Computer Assistant; and 1550, Computer Scientist. Other positions not necessarily in one of these series but with significant AIS responsibilities, such as personnel responsible for AIS security, shall also be designated as AIS positions. Duties involving use of a computer or access to an AIS, by themselves, do not automatically make a position an AIS position.

4-12. Because of uniqueness, special responsibilities, or the need for uniformity throughout DOT, positions in the following categories shall be designated at least at the risk levels shown, regardless of the level determined under the other criteria and procedures of this chapter.

Category of Position	Position Risk Level Shall be at Least
a. Senior Executive Service or a comparable pay.	High Risk
b. Executive Development Program	High Risk
c. Employee is responsible at the national headquarters level for the development and/or approval of national plans, policies, or programs for continuity of a DOT administration's operations during national emergencies.	High Risk
d. Manager responsible for the conduct of accident investigations and/or the enforcement standards through the certification/inspection process.	High Risk
e. Imprest fund cashier or alternate cashier responsible for a fund in excess of $20,000.	High Risk
f. Imprest fund cashier or alternate cashier responsible for a fund in excess of 2,000 but no more than $20,000.	Moderate risk
g. Contracting officer or specialist who has sole, final authority to approve contracts in excess of $1,000,000 in value, or acquire or dispose of land or facilities in excess of $1,000,000 in value, when the approval or other action is not subject to any higher-level approval or concurrence.	High risk

Category of Position	Position Risk Level Shall be at Least
h. Contracting officer or specialist who has sole, final authority to approve contracts up to $1,000,000 in value, or acquire or dispose of land or facilities up to $1,000,000 in value, when the approval or other action is not subject to any higher-level approval or concurrence.	Moderate risk
i. Budget officers in headquarters, regions, and centers.	High risk
j. Budget analysts in headquarters, regions, and centers.	High risk
k. Employee is responsible at the regional center, or headquarters level for overall management of: (1) An activity's property accountability system, to include the conduct of property inventories and the governing of survey boards; (2) acquisition and disposal of lands or DOT facilities;(3) contracting and the issuing of grants; and (4) accounting and/or disbursing of Government funds.	High risk

Chapter 5

PERSONNEL SECURITY INVESTIGATION REQUIREMENTS

5-1. This chapter prescribes minimum investigative requirements and procedures for exceptions to those requirements. The position risk or sensitivity level, and in some cases the security clearance required of a person holding the position, govern the type of investigation required.

Section 1 - Types and Scope of Background Investigations

5-2. Standard investigations. OPM will conduct the following investigations for DOT:

a. National Agency Check (NAC)

b. National Agency Check and Inquiries (NACI)

c. National Agency Check with Law Enforcement Inquiries and Credit (NACLC)

d. Child Care National Agency Check and Inquiries (CNACI)

e. Access National Agency Check and Inquiries (ANACI)

f. Minimum Background Investigation (MBI)

g. Limited Background Investigation (LBI)

h. Background Investigation (BI)

i. Single Scope Background Investigation (SSBI)

j. Reimbursable Suitability/Security Investigation (RSI)

k. Periodic Reinvestigation (PRI)

l. Periodic Reinvestigation with Residence Coverage (PRIR)

m. Periodic Reinvestigation for Single Scope Background Investigation (SSBI-PR)

n. Upgrade Investigation (SGI, BGI, LGI). The SGI upgrades a BI to an SSBI; the BGI upgrades an LBI to a BI; and the LGI upgrades an MBI to an LBI.

o. Update Investigation (SDI, BDI, LDI). The SDI updates an SSBI; the BDI updates a BI; and the LDI updates an LBI.

5-3. Special Agreement Checks (SAC). OPM will conduct SAC's to provide specific types of coverage tailored to an agency's needs.

5-4. Minimum Coverage. All investigations will cover the most recent three years of a person's life. They will not normally extend back beyond his or her 16th birthday unless necessary to obtain a minimum of three years of coverage or to resolve an issue.

5-5. Personal Interview. OPM will conduct one or more interviews of the person who is the subject of the investigation in all SSBI, BI, LBI, Upgrade, SSBI-PR, and PRI cases.

5-6. Credit Searches. OPM will conduct credit searches as part of the NACLC, ANACI, MBI, LBI, BI, SSBI, PRI, SSBI-PR, SGI, BGI, LGI, SDI, BDI, and LDI.

5-7. Expanded Coverage. OPM will expand all background investigations in scope and coverage as necessary to resolve an issue.

5-8. Extra Coverage.

a. If it is appropriate to the position, the servicing security organization may request extra background investigation coverage of the following attributes. OPM investigators will then ask persons they interview additional questions about the subject in order to cover them:

(1) Managerial/supervisory attributes, which include ability to speak and write clearly and concisely; scope, quality, and extent of supervisory experience; ability to get people to work together effectively; resourcefulness; initiative; adaptability; judgment; discretion; ability to cooperate with co-workers, supervisors, and subordinates; and possible conflicts of interest.

(2) Public contact attributes, which include ability to meet and deal with all types of people, diplomacy, tact, personal appearance, and speaking ability.

(3) Law enforcement attributes, which include ability to react to emergencies and conditions of stress, maturity, stability, judgment, and discretion.

(4) Outside the United States attributes for subject and spouse, which

include ability to represent the Government favorably; ability to meet and deal successfully and to adjust to a foreign environment; and whether there are any prejudices, defects in judgment, personal problems, traits, or weaknesses that might discredit the United States should the person be stationed in a foreign country.

b. A servicing security organization may negotiate with OPM for other special coverage in a background investigation if warranted by the position or by known suitability or security issues.

Section 2 – Basic Investigative Requirements

Outlined below are the minimum investigative requirements for all positions within DOT:

5-9. Special-sensitive position. A person in a special-sensitive position shall have a completed SSBI. The investigation shall be completed, evaluated, and favorably adjudicated for both suitability and security before the person is placed in the position, unless this requirement is waived in accordance with Section 4 of this chapter.

5-10. Critical-sensitive position. A person in a critical-sensitive position shall have a completed BI or SSBI. The investigation shall be completed, evaluated, and favorably adjudicated for both suitability and security before the person is placed in the position, unless this requirement is waived in accordance with Section 4 of this chapter.

5-11. Noncritical-sensitive position. A person in a noncritical-sensitive position shall have a completed ANACI or higher-level investigation. If possible, the investigation should be completed, evaluated, and favorably adjudicated for both suitability and security before the person is placed in the position. However, with the servicing security organization's approval, the person may be placed in the position prior to completion of the ANACI. Before giving its approval, the security organization shall review the current SF 86, Questionnaire for National Security Positions; and, if available, the person's employment application and a current OF-306, Declaration for Federal Employment. If the person is a DOT employee, the security organization shall also ensure review of any current PSF. If the person provides information on the SF-86, OF-306, and/or employment application that might indicate a security or suitability issue, the security organization shall not approve the person's placement in the position unless it has conducted appropriate checks, and an interview with the individual, if necessary, to resolve any issues. If the person has a completed NACI, it is only necessary to initiate a credit check before the person is placed in the position.

5-12. High risk position. A person in a high-risk position shall have a completed BI or SSBI. If possible, the investigation should be completed, evaluated, and favorably adjudicated

before the person is placed in the position. However, the servicing human resources organization, in consultation with the servicing security organization, may approve a person's placement in a high-risk position prior to completion of a BI. At a minimum, the security organization shall have reviewed the SF 85-P, Questionnaire for Public Trust Positions, and any other forms that the person might have completed prior to the human resources organization giving its approval, and should have initiated the BI. In no event shall the BI be initiated any later than 14 days after the person is placed in the position.

5-13. Moderate risk position.

a. A person in a moderate-risk position shall have a completed NACI or higher level investigation. If possible, the investigation should be completed, evaluated, and favorably adjudicated before the person is placed in the position. However, the servicing human resources organization, in consultation with the servicing security organization, may approve a person's placement in a moderate risk position prior to completion of the investigation. At a minimum, the security organization shall have reviewed the SF 85-P and any other forms that the person might have completed prior to the human resources organization giving its approval, and should have initiated the investigation. In no event shall the investigation be initiated any later than 14 days after the person is placed in the position.

b. A person in a moderate risk position with fiduciary responsibilities shall have a completed NACI or higher-level investigation. The servicing security organization shall also conduct a credit check on the person or have OPM do one along with the NACI. Positions with fiduciary responsibilities include, but are not limited to, contracting officers, contract specialists, cashiers, and other positions where the incumbent has a major responsibility involving authority or ability to obligate, control, or expend public money or items of monetary value. If possible, the investigation should be completed, evaluated, and favorably adjudicated before the person is placed in the position. The servicing human resources organization, in consultation with the servicing security organization, may approve a person's placement in such a position prior to completion of the investigation. Before doing so, however, the security organization shall have reviewed the results of a current credit check and advised the human resources organization of any information raising a question about the person's financial responsibility. The security organization shall also have reviewed the SF 85-P, and any other forms that the person might have completed prior to the human resources organization giving its approval, and should have initiated the investigation. In no event shall the investigation be initiated any later than 14 days after the person is placed in the position.

5-14. Low risk position. An NACI is required for a person in a low risk position. This investigation shall be initiated within 14 days after the person is placed in the position. Upon completion, the NACI shall be evaluated and adjudicated as soon as possible.

5-15. Periodic Reinvestigations (SSBI-PR, PRI, and NACLC). An SSBI-PR shall be completed on each incumbent of a special-sensitive position, and on each incumbent of a critical-sensitive position for which the person is required to hold a Top Secret clearance, within five years from the date of the last SSBI, BI, or SSBI-PR. A PRI shall be completed on each incumbent of a critical-sensitive position with no Top Secret clearance requirement, and on each incumbent of a high-risk position within five years from the date of the last BI or PRI. The PSF and the OPF shall be reviewed as part of the PRI. In addition, a NACLC shall be completed on each person holding a Secret clearance within 10 years from the date of the last investigation or reinvestigation; and a NACLC shall be completed on each person holding a Confidential clearance within 15 years from the date of the last investigation or reinvestigation.

5-16. Credit checks for fiduciary positions. A credit check shall be conducted on all persons employed in positions with fiduciary responsibilities at least once every five years, regardless of other investigation requirements that may apply. If a person is being placed in one of these positions and no pre-placement investigation is required, or if such a requirement is waived, a credit check shall be initiated as soon as possible, but no later than 14 days after placement. If a credit check has been conducted within the last five years as part of another investigation, a new one is not required.

5-17. Upgrade Investigations. The appropriate Upgrade Investigation (SGI, BGI, or LGI) may be conducted when an MBI, LBI, or BI has been completed within the past five years and the next higher level investigation is now required because an employee is being promoted or reassigned to a position with a higher risk or sensitivity level than the one he or she currently occupies. This investigation is in lieu of the required investigation.

5-18. Update Investigations. The appropriate Update Investigation (SDI, BDI, or LDI) may be conducted in lieu of the required investigation whenever an LBI, BI, or SSBI has been completed within the past five years, the same level investigation is now required, and the person has had a break in Federal service of more than 24 months.

5-19. Equivalent investigations. A combination of investigations or checks that provides coverage equivalent to a required investigation is sufficient to meet the requirement. For example, a completed NACI from OPM and a credit check that the security organization conducts separately will suffice to meet the requirement for an ANACI for noncritical-sensitive positions.

5-20. Investigations on former Federal employees. The investigation required for a position shall be conducted on any former Federal employee who has had a break in service in excess of 24 months. If the person has had no break in service in excess of 24 months, no new investigation is required unless a periodic reinvestigation requirement applies. In determining continuity of service, any one or a combination of the following employments may be credited the same as Federal employment:

a. Active duty in any branch of the U.S. military service.

b. Employment for or as a U.S. Government contractor for which the person had a security clearance granted by a Government agency. Any period of time during which the clearance was not in effect would constitute a break in service.

c. Employment by the District of Columbia Government.

5-21. Changes in risk or sensitivity level. When the risk or sensitivity level of a position changes, an incumbent may remain in the position, but any new investigation required for the new risk or sensitivity level shall be initiated within 14 days of that change.

5-22. Movement from a public trust position to a national security position. An employee moving from a public trust to a national security position shall complete a SF 86, Questionnaire for National Security Positions, which the servicing security organization shall review before placement. If the employee has received the required investigation for the national security position, no reinvestigation is required unless the time elapsed since the previous investigation necessitates updating, or unless information disclosed on the newly completed SF-86 or other special circumstances justify additional investigation.

5-23. Incomplete investigations. An investigation received from OPM that is substantially complete, even if not entirely complete, may be adjudicated for both suitability and security if the servicing security organization determines that the outstanding portion is not likely to affect a final adjudication or help to resolve any issues. Such an investigation may be considered complete for the purpose of meeting a pre-placement investigation requirement.

Section 3 - Exceptions to Investigative Requirements

5-24. Exempt Positions.

a. Certain low risk positions are exempt from the investigative requirements. This exception shall not be viewed as a prohibition from processing the person under the normal investigative requirements. Persons appointed without investigation shall not have access to classified information or to areas restricted for security reasons.

b. The exempt positions are:

(1) Intermittent, seasonal, per diem, or temporary, in which a person's employment does not exceed an aggregate of 180 days in either a single continuous appointment or series of appointments.

(2) Positions located outside the United States that are occupied by persons who are not U.S. citizens.

5-25. Detailed Positions. Individuals occupying permanent positions who are detailed formally or informally into special-sensitive, critical-sensitive, noncritical-sensitive, high risk, or moderate risk positions must meet the normal investigative requirements prior to the detail if the detail is to be in excess of 120 days. If access to classified information is required, the person must have the investigation required for the clearance, or the servicing security organization must be able to grant him or her a temporary clearance under the provisions of Chapter 9, Section 6. If the detail is to a special-sensitive, critical-sensitive, or high-risk position and will be for less than 120 days, the servicing security organization shall review the prior investigation, OPF, PSF, and a current SF-86 or SF-85P, Questionnaire for Public Trust Positions, and SF-85P-S, Supplemental Questionnaire for Selected Positions, as applicable. If a detail originally scheduled for 120 days or less is unexpectedly extended for another period of 120 days or less, the individual may continue in the position without meeting the normal investigative requirements. However, no person may be continued in a series of details in excess of 240 days unless the required investigation is in progress or the requirement is waived in accordance with Section 4 of this chapter.

5-26. Individuals occupying noncritical-sensitive and moderate-risk positions under previously existing requirements. Employees occupying noncritical-sensitive and moderate-risk positions who were investigated under requirements in effect prior to the date of this order and who do not meet the current minimum investigative requirements for positions at these levels may remain in their positions, or be placed in other positions in the same job series and at the same risk or sensitivity level, without further investigation. Noncritical-sensitive employees who hold Secret clearances are subject to the reinvestigation requirement as stated in paragraph 5-15.

Section 4 - Waiver of Pre-placement Investigative Requirements for Special-Sensitive and Critical-Sensitive Positions

5-27. E.O. 10450 requires that waiver of the pre-placement investigative requirements on persons entering sensitive positions may be made only "in case of emergency" provided the department or agency concerned finds that such action is necessary in the national interest. At DOT only M-40 or a servicing security organization with specific delegation from M-40 may grant waivers for persons entering special-sensitive or critical-sensitive positions.

5-28. Prior to appointing a person to a special-sensitive or critical-sensitive position, and prior to making a firm starting date commitment to a person to begin working in such a position, the responsible human resources organization or employing office appointing official shall obtain authorization from the servicing security organization and assurance that either the pre-placement investigative requirements have been met or that the appropriate security organization has granted a waiver. If, through clerical or other error, a person has been permanently appointed to such a position without first meeting the investigative requirements, the human resources organization or employing office shall contact the security organization.

5-29. An office that wants to employ a person in a special-sensitive or critical-sensitive position prior to completion of the required investigation shall submit a written request to the security organization for a waiver of the pre-placement investigative requirement. This request shall include the position's title, grade, and location; a justification of the emergency situation (e.g., critical operational impact if the individual cannot be placed in the position at the present time or by a particular date); the level of security clearance required; and a statement that the person will not have access to classified information until the required investigation is completed and the servicing security organization has granted the necessary clearance.

5-30. The servicing security organization shall:

a. Review the employing office's request for inclusion of all required information, including sufficient justification.

b. Obtain and review the candidate's completed SF-86 and, as appropriate, OF-306; and employment application.

c. Conduct subject interview covering, but not limited to, past and present employment, education, and residences; arrests and convictions; use of alcohol and illegal drugs; mental health; and financial responsibility. The subject shall also be asked if there is anything in his/her background that could raise any questions of personal character or loyalty to the United States. The interviewer should use the questions on the SF-86 as a guide in conducting the interview and should ask the subject about any information furnished on the SF-86, OF-306, or employment application that is not entirely favorable. The interview may be conducted telephonically when the candidate is not readily available for one in person.

d. Conduct a credit check.

e. If the candidate is a current or former DOT employee, review the OPF (current

employee) and PSF, if available. If the person is currently employed outside the security organization's area of responsibility, contact the appropriate organization for the OPF and PSF reviews.

f. Conduct a check of the current or former employing agency's security office (for current and former Federal employees only), if other than DOT.

g. Initiate the required investigation.

h. If the security organization believes that the request for waiver should be approved, forward all pertinent information, including copies of the employing office's request and the person's SF-86, to M-40 or the security organization with delegated authority to approve the waiver request.

5-31. In processing a waiver, the servicing security organization may conduct appropriate local law enforcement agency checks that are readily available. For current or former Federal employees, it may wish to conduct a check of OPM's SII, especially if information from a former agency's security office appears incomplete.

Section 5 - Financial and Foreign Travel Disclosure Requirements

5-32. The Director, M-40, may designate positions or categories of positions within DOT that require the incumbents to provide financial disclosure statements and relevant foreign travel information as necessary to comply with Section 1.3 of E.O. 12968. Any statements or information to be provided would be as developed or determined by the Security Policy Board and implemented throughout the Executive Branch.

5-33. Before obtaining a report from a credit reporting agency concerning an individual, or initiating any investigation that will include obtaining such a report, the servicing security organization shall provide the individual written notice that a credit report may be used for employment purposes and shall obtain written authorization from the individual to obtain the report. As required by 15 U.S.C. 1681b, this notice and authorization shall be in a document consisting solely of the notice and authorization. The security organization may use DOT Form 1631, Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act, or a comparable form, to meet this requirement.

Section 6 - Investigative Requirements for Non-Federal Personnel

5-34. Appendix 2, Investigating Contractor Employees, contains the investigative requirements for DOT contractor personnel who do not need access to classified information.

5-35. Appendix 3, NISP contains the policy and procedures for implementing the NISP at DOT. The procedures apply whenever contractors, contractor employees, consultants, or other persons performing work for or under the direction of DOT require access to classified information in order to perform their duties.

5-36. Appendix 4, Investigating Child Care Services Workers, contains the policy and procedures for conducting background investigations on persons working in DOT-sponsored child care centers as either employees or volunteers.

Section 7 – Forms

5-37. When initiating investigations on DOT employees and applicants, servicing security organizations shall use the forms prescribed for the sensitivity or risk level of the individual's position: the SF-86 for national security positions (special-sensitive, critical-sensitive, and noncritical-sensitive); the SF-85P and the SF-85P-S, as applicable, for public trust positions (high risk and moderate risk); and the SF-85, Questionnaire for Nonsensitive Positions, for low risk positions. A completed SF-87, Fingerprint Chart, shall be submitted for all DOT employee and applicant fingerprint checks. The SF-86A, Continuation Sheet for Questionnaires SF-86, SF-85P, and SF-85, may be used as necessary. The servicing security organization may request the individual to submit other forms, such as the DOT Form 1631 or the OF-306, as necessary to meet legal or investigating agency requirements.

Chapter 6

RECIPROCITY AND STANDARDS FOR USING PREVIOUS INVESTIGATIONS

Section 1 - General

6-1. Some applicants for DOT employment and some newly hired employees, especially those persons transferring from other Government agencies, will have already been investigated by another Federal department or agency. Servicing security organizations shall use these investigations when practicable to reduce the number of investigations that DOT requests from the OPM or conducts itself, thereby reducing investigative costs and delays in waiting for investigations to be completed.

6-2. Previously conducted background investigations shall not be duplicated when those investigations meet the scope and standards for the level of a security clearance required. Servicing security organizations granting clearances to civilian and/or military personnel are responsible for determining whether such individuals have been previously cleared or investigated by the U.S. Government. Any previously granted security clearance that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance shall provide the basis for issuance of a new clearance without further investigation or adjudication.

6-3. Previously conducted investigations and access adjudications shall be mutually and reciprocally accepted by all DOT organizations without requiring additional investigation, unless there has been a break in the individual's Federal employment or military service in excess of two years or unless the servicing security organization is aware of unfavorable information about the person that might affect a security adjudication and that was unknown at the time of the previous investigation. This requirement does not apply if a previous clearance was an interim or temporary one and was not based on a completed investigation of the type required for a final clearance at that level.

6-4. In reviewing an employment application; an SF-86, Questionnaire for National Security Positions; an SF-85P, Questionnaire for Public Trust Positions; or an SF-85, Questionnaire for Nonsensitive Positions, a security organization should be alert to any information indicating that the applicant may have had a previous investigation. Such information would include recent Federal employment; military service, including service with the National Guard or reserves; employment with a Government contractor where the person might have held a security clearance; and a claim by the person that he or she has had a previous investigation and/or a security clearance.

6-5. When a previous investigation is readily available, the security organization should review it prior to giving a human resources organization or employing office permission to

employ the person in a sensitive (special-sensitive, critical-sensitive, or noncritical-sensitive) position, or before a human resources organization employs a person in a public trust (high risk or moderate risk) position. If possible, the security organization should obtain a copy of the investigation for the person's PSF.

6-6. If a previous investigation is not readily available, the security organization should obtain as much information as possible about it before the person is employed in a sensitive or public trust position. Sources of this information can include the agency that conducted the investigation, an employing agency security office, or an agency that granted the person a security clearance. The security organization should request a copy of the investigation and review it as soon as possible.

6-7. An investigation that another Federal agency conducted on a DOT applicant or employee, and that is of the same type and scope as the one required for the DOT position, is sufficient to meet the investigative requirements provided that it was conducted within the past two years or that the applicant or employee has had no break in service in excess of two years since the investigation was completed. Except where there is substantial information indicating that an individual may not meet the suitability and/or security standards and criteria stated in Chapter 3, such an investigation shall be accepted by DOT. Any higher-level investigation than the one required for the position also meets the requirements.

6-8. An investigation conducted by a state or local Government agency may provide useful information, particularly in determining whether or not to waive a pre-placement investigative requirement. However, such an investigation, regardless of how extensive it is, does not meet investigative requirements for Federal employment.

Section 2 - Obtaining and Reviewing Previous Investigations

6-9. Office of Personnel Management. OPM maintains the SII, an index of investigations conducted by OPM and certain other Federal agencies. A servicing security organization shall check this index, maintained at OPM's Federal Investigations Processing Center (FIPC), Boyers, Pennsylvania, whenever there is an indication that OPM or another agency has conducted an investigation.

a. National Agency Check and Inquiries Investigations. The method of documenting NACI's depends on when they were completed. When sending a completed NACI to an agency, OPM furnishes a certificate that an agency security officer or specialist signs and that then is placed in an employee's OPF. If a DOT applicant or employee previously worked at another agency, this certificate in the OPF provides sufficient documentation that the NACI was completed on the date shown. Prior to instituting this procedure, OPM returned a copy of the person's employment application

stamped either "Processed under 3(a) of E.O. 10450," or "Results furnished to requesting agency." Either of these stamps on an employment application in an applicant's or employee's OPF also provides sufficient documentation that an NACI was completed. An employment application stamped "Processed under 3(a) of E.O. 10450" indicates that the NACI results were favorable. An employment application stamped "Results furnished to requesting agency," or a certificate showing completion of an NACI, indicates that OPM did not adjudicate the results, but instead sent them to the agency for adjudication. In these cases, the security organization shall check with whichever sources are available to determine whether or not the NACI revealed any information raising security or suitability issues. These sources may include FIPC or the appropriate agency security office.

b. Other investigations. When an SII check or other documentation reveals that OPM previously conducted another type of investigation, the security organization shall obtain and review a copy of that investigation.

6-10. Department of Defense.

a. DOD indexes its investigations in the DCII, maintained by the DSS. These include investigations on military personnel, DOD civilian employees, and DOD contractor personnel.

b. The Defense Industrial Security Clearance Office (DISCO), an office of DSS, grants security clearances to contractor employees. A security organization may conduct name checks with DISCO, in Columbus, Ohio, to obtain investigation and security clearance information. Copies of investigations conducted for DISCO clearances may be requested through DCII.

6-11. Federal Bureau of Investigation. To request a check of the FBI's investigations index, and a copy of any report of investigation the FBI might have, the security organization should prepare DOT Form 1600.14, FBI Record Check Request. The servicing security organization should mark the block at the top of the form titled, "FBI Name Check," and should mail the completed form to: U.S. Department of Justice, Federal Bureau of Investigation, Records Branch, Washington, DC 20535.

6-12. Other Federal Agencies. Other Federal agencies have authority, either by law or through agreement with OPM, to conduct their own investigations pursuant to Executive Order 10450. These agencies include Department of State (DOS), Central Intelligence Agency, Peace Corps, U.S. Secret Service, Internal Revenue Service, U.S. Customs Service, and U.S. Postal Service. If an applicant or employee has been employed by one of these agencies, or if there is an indication that one of them conducted an investigation on the person, the security organization should contact the agency security office for a check of its files and to obtain a copy of any report that the agency might have. If there is any indication

that a copy of an investigation might be on file at OPM, FIPC, the security organization may request a copy as it would for an OPM investigation. OPM will furnish a copy of another agency's investigation if it has it on file and if it meets current OPM criteria for release.

Chapter 7

ROLE OF SECURITY IN SUITABILITY ADJUDICATION

7-1. DOT human resources organizations are responsible for suitability adjudication for both applicants and employees. Employees not subject to suitability determinations under the provisions of 5 CFR Part 731 are subject to disciplinary and removal actions under other authorities. Human resources organizations work with employing offices in taking these actions.

7-2. Employment applications and related paperwork, such as an OF 306, Declaration for Federal Employment, may reveal information raising a question about an applicant's suitability for employment. Human resources organizations should consult with their servicing security organization in these cases regarding the type of investigation necessary to resolve the suitability issue(s). The security organization may initiate the investigation required for the position or a higher-level investigation than the one that is required. In the event of a serious issue that may preclude hiring the person based on the information that the applicant has provided, the security organization may conduct a limited inquiry in an effort to quickly resolve an issue, such as by obtaining court, credit, or other record information.

7-3. In many cases suitability issues will not be evident until the required background investigation is completed or obtained by DOT, either while a person is still an applicant or after being hired. The servicing security organization will receive all investigative reports from OPM and in some cases will receive reports of investigation completed by other agencies. The security organization shall also provide a person the opportunity to respond to unfavorable information when required by paragraph 2-3. While investigating issues involving employee conduct, security organizations may also receive information that could warrant an unfavorable suitability determination.

7-4. When a security organization has information that may warrant an unfavorable suitability determination, it shall forward all reports and pertinent information to the human resources organization for adjudication. The security organization may forward any reports of investigation to the human resources organization, but is not required to do so when they contain no unfavorable information or information that could not reasonably be expected to result in an unfavorable suitability determination. However, the security organization should forward to the human resources organization any reports or other information that might raise a question about an individual's qualifications for a particular job, even if they raise no suitability or security issue.

7-5. If a person is an applicant for a position requiring the incumbent to have access to classified information, the security organization may, if warranted, deny granting the security clearance required for the position. In doing so, the security organization shall follow the procedures in chapter 10, in addition to providing the human resources organization with all information necessary to make a suitability determination. The security organization would normally take this action after the human resources organization has made a favorable

suitability determination. Except as specified in paragraph 7-7, the human resources organization may make a suitability determination even if the security organization has not made a security determination or completed all of the actions required under chapter 10. An applicant denied a clearance required for a position shall not be appointed to the position.

7-6. If a person is an employee in a sensitive position, the security organization may, if warranted, revoke any security clearance required for the position, provided that it does so following the procedures in Chapter 10. It shall also provide the human resources organization with all information necessary to make a suitability determination or take other adverse personnel action as may be warranted. The security organization may revoke the clearance even if the human resources organization has not made a suitability determination or taken any other action; and, except as specified in paragraph 7, the human resources organization may make a suitability determination even if the security organization has not completed all of the revocation actions required under Chapter 10.

7-7. A human resources organization shall not make an unfavorable suitability determination for the purpose of denying an employee full due process following a proposed security clearance revocation, or denying him/her an opportunity to appeal a clearance revocation to the Personnel Security Review Board (PSRB), (See chapter 10). Neither the human resources organization nor the employing office shall take an adverse personnel action based on an employee being denied a security clearance, or having a security clearance revoked, until the Review Board has made a final decision on any appeal that the employee has filed.

7-8. Upon request of OPM, DOT is required to report to OPM on the final adjudicative action based on an OPM report of investigation or a file OPM furnishes in response to a check of its SII. Security organizations shall work with the human resources organizations they service to ensure that OPM forms used for this purpose are completed and returned to OPM. If a security organization makes an adverse security determination, which precludes any suitability adjudication, it shall complete the applicable OPM form and return it to OPM.

Chapter 8

SECURITY ADJUDICATION

8-1. E.O. 10450, Security Requirements for Government Employment, requires that an agency make a security determination as to whether the employment of each civilian officer or employee is clearly consistent with the interests of the national security. E.O. 12958, Classified National Security Information, and E.O. 12968, Access to Classified Information, require that a determination be made concerning whether a person is eligible for access to classified information. Servicing security organizations are responsible for adjudicating all pertinent information and making these determinations. Chapter 9, Access to Classified Information, contains more specific criteria and procedures for granting access to classified information. Appendix 1, Security Adjudication Guidelines, contains specific guidelines for determining eligibility for access to classified information.

8-2. The servicing security organization, consistent with delegated authority from M-40, is responsible for security adjudication for all employees and applicants for positions under its jurisdiction. However, it shall not adjudicate cases on its own manager or on any of its personnel directly responsible for administering the personnel security program.

8-3. Cases that raise significant questions regarding a person's loyalty to the United States and cases where the servicing security organization manager concludes that a person has been coerced, influenced, or pressured to act contrary to the interests of the national security shall be referred to M-40, which will then refer them as appropriate to the FBI.

8-4. During initial review of any report of investigation or of any information received that raises a security issue, the servicing security organization shall:

a. Determine if there are any material gaps in coverage of the individual's activities.

b. Determine if there are any significant discrepancies between activities claimed on an SF-85, SF-85P, SF-85P-S, SF-86, OF-306, or employment application, and those shown in the report or other information received.

c. Decide if there is any questionable medical information requiring an opinion of. competent medical authority

8-5. The servicing security organization shall obtain additional information as needed to adjudicate the case. It may request the OPM to conduct additional investigation if an OPM report appears to be inconclusive or incomplete, or to conduct a RSI to resolve an issue raised in a NACI Investigation or MBI. The security organization may also, however, initiate an investigation of its own or inquiry to resolve any issues. By personal interview or interrogatory, the security organization may question an

applicant or employee about discrepancies relating to applications or security forms, but may not allow the person to amend such forms to eliminate the discrepancies.

8-6. The security organization shall assess all issues in question (except loyalty cases) in terms of the sensitivity of the duties and responsibilities of the position and whether any conduct in question indicates that employment of the person in a sensitive position and granting of access to classified information if applicable would pose a risk to the national security. Any conduct indicating that the person, through individual or collective action or inaction, may impair the security interests of the United States demonstrates a national security risk. The standard and criteria to be used in this assessment are those stated in Chapter 3, Section 2. The guidance in Appendix 1 shall be used in all determinations of eligibility for access to classified information.

8-7. The security organization shall give particular attention to any indication of unreliability, untrustworthiness, lack of dependability, potential for subornation or blackmail, dishonesty, or disregard for the law or established authority. If the security organization believes that the granting of a security clearance is not clearly consistent with the interests of the national security, it shall deny the applicant or employee a security clearance, following the procedures in Chapter 10. In the case of an employee who already has a clearance, the security organization shall immediately suspend the person's access to classified information, if that has not already been done, following the procedures in Chapter 9, paragraph 9-36. It shall then initiate the process for revocation of the clearance, following the procedures in Chapter 10, Section 2. If the security organization believes information warrants suspension or removal of an employee under the provisions of 5 U.S.C. 7532, it shall follow the procedures in Chapter 10, Section 3.

8-8. In the interests of national security, DOT, and the individual involved, the security organization shall adjudicate cases promptly.

8-9. The security organization shall maintain a record of all security adjudications, to include copies of any forms returned to OPM that document the adjudication.

8-10. When the security organization proposes an adverse security action, it shall maintain, at a minimum, an administrative due process file (which may be included as part of the PSF) consisting of the documents mentioned in paragraph 8-9 and the following:

a. Copies of all communications sent to the individual.

b. Copies of all written challenges, replies, or documentation supplied by the individual, to include a written summary of any oral response.

c. A copy of any report of investigation from OPM, another agency, or a DOT organization.

d. Copies of any other documents related to the case.

8-11. When the individual is an applicant and does not become a DOT employee, the file created when an adverse security action is proposed shall be retained for at least two years from the date of the final decision in the case. If no adverse action is proposed on an applicant who is never hired, the security organization shall keep the record of the adjudication for at least one year from the date of the adjudication. If the person is or becomes a DOT employee, the security organization shall include the above documents in the PSF.

Chapter 9

ACCESS TO CLASSIFIED INFORMATION

Section 1. General

9-1. Access authorizations are certifications by servicing security organizations in accordance with provisions of E.O. 12958 and E.O. 12968 that persons are found to be sufficiently trustworthy to be allowed access on a need-to-know basis to classified national security information at specified levels. These authorizations are generally called security clearances. Servicing security organizations may grant them for access to classified information at the Confidential, Secret, and Top Secret levels.

9-2. Except as provided in Section 11 of this chapter, security organizations shall grant access only to employees who are United States citizens on whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicate loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. In granting access to classified information, the security organization shall apply the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, guidelines that the President approved in March 1997 for use throughout the Executive Branch. Appendix 1 contains these guidelines.

9-3. A determination of eligibility for access to classified information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate that access to classified information is clearly consistent with the national security interests of the United States. Any doubt shall be resolved in favor of the national security.

9-4. In granting access to classified information, security organizations shall not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation.

9-5. Employees shall not normally be granted access to classified information unless they have been determined to be eligible for access based upon a favorable adjudication of an appropriate investigation of their background, have a demonstrated need-to-know, and have signed an approved nondisclosure agreement. In very exceptional circumstances, where official functions must be performed prior to completion of the investigative and adjudicative processes, an interim clearance or temporary access may be granted. At any time during the period individuals are required to have access to classified information, they may be required

to undergo a reinvestigation to ascertain whether they continue to meet the requirements for access to classified information.

9-6. Access authorizations shall be terminated when no longer required.

9-7. Especially tight controls are imposed in processing Top Secret access authorizations and requests for access to SCI. DOT does not have authority to grant access to SCI, but the Director of Central Intelligence may grant such access to a DOT employee when necessary for the employee to perform his or her duties.

Section 2 - Limitations and Restrictions on Access to Classified Information

9-8. The level of access approved for an employee shall be limited, and relate directly to the level of classified information the employee has a need to access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

9-9. No one will be eligible for access to classified information merely because of Federal service, contracting, license, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of their title, rank, position, or affiliation.

9-10. The number of persons cleared for access to classified information shall be kept to a minimum, consistent with the requirements of operations. A security clearance shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access to classified information and such access can reasonably be prevented. Security clearances should not be issued to:

a. persons in non-sensitive positions;

b. persons whose regular duties do not require access to classified information;

c. persons within a restricted, controlled, or industrial area, who do not require access to classified information;

d. persons who may only have inadvertent access to sensitive information or areas, such as emergency service personnel, firemen, doctors, nurses, police, mailroom employees, or similar personnel;

e. persons who can be prevented from accessing classified information by being escorted by cleared personnel;

f. maintenance or cleaning personnel, including persons who perform maintenance on office equipment such as computers and photocopiers, who only have inadvertent access unless such access cannot be reasonably prevented; or

g. perimeter security personnel who have no access to classified information.

9-11. Eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

9-12. Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need to know that information.

Section 3 - Request Procedures

9-13. The servicing security organization shall grant a security clearance only upon specific written request from the employee's supervisor or a manager for whom the employee works or when the need for a clearance for the position has been documented. This request or other documentation shall specify the reason that a clearance is necessary and the level of classified information to which the employee will need access.

9-14. If the employee will not need access to classified information for a period of time exceeding six months, the supervisor or manager should request a temporary clearance for the required amount of time.

9-15. When requesting an interim clearance, the supervisor or manager shall specify the reason that the clearance should be granted before the expected completion date of the required investigation and the consequences of not waiting for the investigation to be completed.

9-16. When appropriate, and in lieu of submitting a separate request for each employee needing a clearance, a supervisor or manager may submit a request for clearances that covers an entire group of employees, such as all of those persons working in his or her organization who occupy a particular position or positions, or all employees working at a particular facility or in a specified office. Such a request shall then be sufficient for the security organization to grant clearances to all employees in the specified group(s). Position sensitivity designations should be reviewed as clearances are requested in order to ensure that positions have the appropriate sensitivity levels required and that these levels are adjusted as necessary.

9-17. E.O. 12968 requires that an agency limit the number of employees that it determines are eligible for access to classified information to the minimum required for the conduct of agency functions. Supervisors and managers shall request security clearances for employees only when there is a demonstrated, foreseeable need for access. The security

organization shall evaluate all clearance requests to determine need in accordance with policies stated in the latest edition of DOT Order 1640.4, Classified Information Management. Upon the security organization's request, an office requesting a clearance for an employee shall provide information necessary to confirm that the employee needs access to classified information at the level specified.

Section 4 - Interim Clearances

9-18. In exceptional circumstances where an employee must perform official functions requiring access to classified information prior to completion of the required investigation, the servicing security organization may grant the employee an interim security clearance pending completion of the investigation. (E.O. 12968 refers to access under these circumstances as temporary eligibility for access; but this type of clearance is different from a temporary clearance addressed in Section 6 of this chapter.) This type of access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of this access. This process shall not be used in lieu of a waiver or as a means to place an employee in a sensitive position without the required background investigation.

9-19. Upon determining that they are needed and justified, security organizations may grant interim clearances for access to Confidential and Secret information. Only M-40 may grant interim Top Secret clearances.

9-20. Any one of the following may serve as the basis for the security organization to grant an interim Confidential or Secret clearance:

a. Receipt of the advance report of a favorable National Agency Check (NAC) in a current investigation or confirmation of a favorable NAC completed within the preceding one year.

b. Confirmation of a completed DOD NAC on a former member of the armed forces provided that:

(1) The individual has not had more than a two-year break in service between the date he or she was released from the military and the beginning date of the person's DOT employment;

(2) The DOD NAC has been completed during the person's most recent enlistment and within the past six years; and,

(3) The security organization reviews the individual's DD Form 214, Armed Forces Report of Transfer or Discharge, to determine the person's character of service and/or the conditions under which the person was discharged from the military service.

c. Confirmation of a completed NAC that another Government agency used to grant the person a security clearance for employment as or for a Government contractor, provided that:

(1) Not more than two years have elapsed between the date that the clearance was last in effect and the beginning date of the person's DOT employment; and

(2) The security organization has confirmed that the clearance was not revoked for any reason raising a question about the person's fitness to hold a clearance.

9-21. The security organization shall not grant an interim clearance without reviewing the SF 86 and initiating the required investigation.

9-22. As a matter of practice, M-40 rarely grants interim Top Secret clearances. As much of the required investigation as possible shall be completed before this level of interim clearance is requested from M-40. A DOT organization requesting M-40 to grant an interim Top Secret clearance shall include with its request copies of the SF-86 used to initiate the investigation, all available investigative information obtained to date, and any other pertinent information.

9-23. The minimum investigative requirements for an interim Top Secret clearance are as follows:

a. For someone who has already been the subject of a current, favorable investigation, completion and review of the SF-86, including any applicable supporting documentation, and expedited submission of a request for an SSBI.

b. For someone who has not been the subject of a current favorable personnel security investigation of any kind, completion and review of the SF-86, including any applicable supporting documentation, and expedited submission of a request for an SSBI. In addition, the servicing security organization shall ensure completion and favorable review of relevant criminal history and investigative records checks at the FBI, and checks of OPM's SII and the DCII. The results of these checks may be obtained through an advance NAC report from OPM pending completion of the SSBI. Whenever possible, the servicing security organization should also conduct a credit check or obtain the results of one conducted by OPM.

9-24. The servicing security organization shall grant an interim clearance for a period of not more than six months. If the required investigation has not yet been completed at the end of that time, the security organization, after checking on the status of the investigation and the information developed to date, may extend for up to another 6 months the period of time that the clearance remains in effect. A final clearance supersedes an interim clearance.

9-25. Upon being granted an interim clearance, the employee shall complete and sign the SF-312, Classified Information Nondisclosure Agreement, and receive the appropriate briefing. The security organization shall also notify the employee in writing, as E.O. 12968 requires, that further access is expressly conditioned on the favorable completion of the investigation and adjudication of its results. The security organization shall immediately terminate an interim clearance if the investigative results do not warrant the granting of a final clearance.

Section 5 -- Final Clearances

9-26. A servicing security organization may grant a final clearance when the required investigation has been completed and adjudicated and all other pertinent official records have been reviewed and evaluated. The security organization may also grant the clearance when the investigating agency or organization has provided a substantially complete investigation, even though a minor portion is still pending, if in the adjudicator's opinion the completed portion clearly supports a favorable adjudication and the pending information is unlikely to raise a material issue or help to resolve one.

b. The investigative requirements for final clearances are:

(1) Confidential or Secret. Access National Agency Check and Inquiries (ANACI); NACI plus a credit check; or higher level investigation with no subsequent break in service in excess of two years.

(2) Top Secret. SSBI with no subsequent break in service in excess of two years. In using a combination of other investigations, the adjudicator must determine that together they provide investigative coverage equivalent to that of an SSBI.

Section 6 - Temporary Clearances

9-27. Temporary eligibility for access, referred to as a temporary clearance, may be granted when there is a need for an employee to have this access for a limited period of time, such as for one-time participation in a classified project.

9-28. The servicing security organization may grant a temporary clearance to an individual who has met the requirements for an interim or final clearance, except that only M-40 may grant a temporary Top Secret clearance if the person does not have a current BI or SSBI. It is not necessary to initiate an SSBI for the purpose of granting a Top Secret clearance as would be required for an interim or final clearance.

9-29. The security organization shall review a current, signed SF-86 from the individual before granting a temporary clearance.

9-30. The security organization shall grant a temporary clearance for a period of time not to exceed 60 days; but, if circumstances warrant, may then extend it for an additional period of time not to exceed a total of six months. The security organization shall establish a fixed date or event for expiration of the clearance. The access granted shall be limited to information related to a particular project or assignment.

9-31. When an individual is being granted a temporary clearance for access to another agency's classified information, that agency must concur before DOT grants the access. The security organization shall take appropriate steps to ensure that the other agency concurs with the release of its classified information to an employee with a temporary clearance.

Section 7 - Clearance Granting Procedures and Documentation

9-32. Basic procedures.

a. Servicing security organizations shall make all determinations regarding the granting of security clearances and shall document clearances granted. The documentation should include the level and date of clearance, the investigative basis and date of investigation, the sensitivity of the employee's position, and the date of the last update investigation, if applicable. The security organization shall then work with the employing organization to arrange for a security briefing and for the individual to sign SF 312, Classified Information Nondisclosure Agreement. In signing the SF-312, the individual agrees not to disclose to any unauthorized person any classified information the employee has access to during the time that he or she holds a security clearance and at all times thereafter.

b. A person only needs to sign an SF-312 once, regardless of how many times he or she is granted a clearance. Security organizations shall ensure that the employee has received a briefing and has signed the SF-312, and shall then notify the employee's organization in writing -- electronic notification is permissible -- that he or she has been granted a clearance and shall specify the level of clearance granted. The security organization shall send the SF-312 to the servicing human resources organization for placement in the employee's OPF.

9-33. Temporary and interim clearances.

a. An employee being granted an interim or temporary clearance is required to sign the SF-312 and receive a security briefing. The security organization shall document the clearance in writing to the employing office.

b. Whenever an employee has been granted an interim or temporary clearance, the security organization shall convey that fact to any other agency that considers affording the employee access to its information. The security organization

should include this information on any visit request form containing clearance information that it sends to another agency.

9-34. Security briefings.

a. Security briefings shall be given to all persons authorized access to classified information to ensure that they fully understand the requirements and procedures for protecting it, the specific hazards that may be expected, what to do if a compromise occurs, and their continued obligations after their clearances are terminated.

b. A person shall receive a security briefing each time he or she is granted a security clearance, unless the employee has already received a briefing within the past year.

Section 8 - Terminating Access Authorizations

9-35. Administrative termination. The servicing security organization shall administratively terminate an employee's security clearance whenever his or her DOT employment is terminated for any reason or when duty changes occur that eliminate the need for the clearance. When the latter situation exists, the employee's supervisor shall request termination of the clearance or reduction in the level of clearance, if appropriate. Clearance termination or reduction in level may require reassessment of the sensitivity level of the employee's position or re-designation of the position as nonsensitive.

9-36. Clearance suspension. Suspension of a clearance, also known as administrative withholding, is appropriate when a significant question of security fitness arises. Suspension is warranted, for example, when the security organization receives information indicating possible gross misconduct, criminal conduct, substance abuse, or a serious breach of integrity.

a. Clearance suspension is a temporary action and shall be in effect only while a question of security fitness is being investigated, while other pertinent information is being obtained and evaluated, or while legal, administrative, or other action is pending that is expected to have a bearing on whether or not the employee can continue to hold a clearance. It may remain in effect while an employee is participating in a rehabilitation program following determination of substance abuse; or in a rehabilitation program, counseling, or therapy resulting from legal action occurring outside of DOT. The security organization may reinstate the clearance whenever it believes that this action is consistent with the interests of national security, even though the employee is still participating in a rehabilitation or similar program. However, the security organization is not required to do so when other DOT offices, such as a medical office, have determined that the employee is fit for duty. The security organization shall make every effort to

complete all investigations expeditiously and obtain information necessary to make a final determination regarding an employee's clearance; and, when appropriate, shall reinstate a suspended clearance as soon as possible. When the security organization determines that a clearance should be revoked, it shall promptly begin the procedures to do so.

b. Whenever an employee's security clearance has been suspended for a total of 180 days, the servicing security organization shall notify M-40 of the circumstances surrounding the suspension and the action(s) pending that the security organization believes will enable it to make a final decision regarding clearance reinstatement or revocation.

c. When suspending clearances, security organizations shall ensure adherence to the clearance suspension procedures contained in Chapter 10, Section 2.

d. A servicing security organization shall fully coordinate a clearance suspension with the employee's supervisor. While it is not necessary to inform the employing office in detail of the reason for a suspension, the security organization shall notify the office in writing that the clearance has been suspended and shall ensure that the employee is notified. As stated in paragraph 10-6, a clearance suspension exceeding 10 days requires written notice to the employee.

9-37. Security Debriefings. All persons vacating a sensitive position must sign the termination portion of an SF-312 or other approved DOT termination form, which constitutes a security debriefing. The official conducting the debriefing shall sign the form as a witness. The completed form shall be returned to the security organization, which shall retain it for at least one year. This statement is not required when an employee transfers to another sensitive position or when a clearance is suspended, but only when employment with a DOT organization ends, a temporary clearance expires, or the individual permanently transfers to nonsensitive duties.

Section 9 - Special Access Authorizations

9-38. Access to special categories of classified information or special access programs requires additional security adjudication and briefings.

9-39. Requirements for access to SCI are contained in Director of Central Intelligence Directive 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to SCI.

9-40. Department of Energy (DOE) Clearances.

a. DOE issues security clearances for access to DOE Restricted Data under the provisions of the Atomic Energy Act of 1954, as amended. DOE Restricted Data

relate to the design, manufacture, and use of atomic weapons, the production of special nuclear material, and energy production. Restricted Data is assigned classification levels of Confidential, Secret, and Top Secret similar to the levels of other national security information classified under the provisions of E.O. 12958, Classified National Security Information.

b. Each DOT organization maintaining personnel security operations shall obtain and control the DOE clearances for personnel under its jurisdiction. The Director, M-40, or an organization to which M-40 has delegated the responsibility, shall obtain and control the clearances for all other DOT organizations.

c. When an DOT employee needs access to Restricted Data, the employee's management shall request the servicing security organization to arrange for this access. The security organization shall then obtain from the employee any forms that DOE requires and follow DOE procedures in processing the request.

d. The background investigation and reinvestigations requirements for a DOE "Q" clearance are the same as those for a Top Secret clearance. The requirements for DOE "L" clearances are the same as those for Secret and Confidential clearances.

e. The decision to grant or deny a DOE clearance is solely a DOE responsibility, and denial of a clearance is not subject to review or appeal by DOT. DOE is responsible for affording an employee all due process rights as prescribed by E.O. 12968. However, when DOE denies a clearance for a DOT employee, the servicing security organization shall review any information that DOE used in making its decision that was not available when the security organization granted the employee's current DOT security clearance. It shall then determine whether or not the employee's continued access to classified information is clearly consistent with the interests of national security.

f. When DOE grants a Restricted Data clearance and notifies the servicing security organization, the security organization shall notify both the employee and the employing office. Because it is contrary to DOE regulations to provide the employee with written notification of a DOE clearance, the security organization shall provide this notification orally. The security organization shall also ensure that the employee receives all briefings that DOE requires.

g. The security organization shall arrange for termination of a DOE clearance when an employee no longer needs it to perform official DOT duties. It shall ensure that the employee is debriefed according to DOE procedures.

9-41. Access by DOT personnel to North Atlantic Treaty Organization (NATO) classified information requires special authorization by DOT security organizations. The United States Security Authority for NATO prescribes criteria for issuing these authorizations.

a. The Director, M-40, and personnel security officials at the headquarters level in USCG, FAA, and MARAD have authority to issue NATO access authorizations. This authority may be re-delegated to specific operating officials trained in the procedures for granting the authorizations and in conducting the required briefings and debriefings.

b. A request for authorization for access to NATO classified information shall be initiated by an employee's supervisor or other management official who can attest to the official need for it. The request shall specify the level of NATO information to which the employee will need access. NATO information is marked COSMIC Top Secret (in lieu of NATO Top Secret), Secret, and Confidential.

c. A security clearance issued under the provisions of this chapter is a prerequisite for authorizing access to NATO information at the corresponding level. Before the employee is allowed access to NATO information, he or she shall also receive a thorough briefing in the security requirements concerning it. Upon determining that an employee may be granted access to NATO information, the personnel security official shall issue a NATO access authorization specifying the level of access and shall also notify the employee's office.

d. When the employee ceases to be employed in a position requiring access to NATO classified information, the servicing security organization shall debrief the employee regarding his or her continued responsibility to safeguard the information.

Section 10 - Security Clearances for National Defense Executive Reserve (NDER) Personnel and Federal Port Controllers

9-42. The servicing security organization for a DOT organization in which an NDER unit is located shall provide full personnel security servicing for the unit and is responsible for granting necessary security clearances to NDER personnel.

9-43. The servicing security organization for MARAD shall grant security clearances as necessary to Federal Port Controllers who in time of emergency, in order to meet the needs of the national defense and maintain the essential civilian economy as specified in Title 46 CFR Part 346, Federal Port Controllers, would become paid MARAD employees.

9-44. All requirements of this manual in regard to background investigations and the granting of security clearances that apply to DOT employees also apply to NDER personnel and Federal Port Controllers.

Section 11 - Security Clearances and Authorizations for Non-United States Citizens

9-45. Where there are compelling reasons in furtherance of a DOT mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the Director, M-40, be granted limited access to classified information. This access shall only be for specific programs or projects for which there is a need for such access.

9-46. The Director, M-40, is authorized to grant Limited Access Authorizations to non-U.S. citizens. M-40 may not further delegate this authority.

9-47. When a DOT organization believes that compelling reasons exist to grant a Limited Access Authorization, it shall submit a written request to the servicing security organization. The request shall clearly describe the nature of the classified information involved and state the level of classification. The requesting office shall clearly show that the person's services are of such unique quality and character as to be unobtainable elsewhere; and if his or her services are not obtained, the work cannot proceed or will be seriously impaired to the extent that national security interests will be affected. If the servicing security organization concurs with the request, it shall forward it to M-40.

9-48. A BI is the minimum basis for granting a Limited Access Authorization, and such an authorization may be approved only if the prior 10 years of the person's life can be appropriately investigated. The servicing security organization, after consultation with M-40, shall obtain all required investigative forms from the individual, initiate any necessary investigation, and forward the completed investigation to M-40. M-40 shall then determine whether or not to grant the requested authorization. In granting a Limited Access Authorization, M-40 shall specify both the level and the type or category of classified information to which the non-citizen may have access.

9-49. No non-citizen shall be eligible for access to any higher level of classified information than the United States Government has determined may be releasable to the country of which the person is currently a citizen.

CHAPTER 10

ADVERSE SECURITY ACTIONS

Section 1 - General

10-1. This chapter prescribes procedures that DOT personnel shall follow upon receipt of information about an employee or applicant that may result in an adverse security action. Such actions include denial, suspension, or revocation of a security clearance for access to classified information.

10-2. Upon receipt of information that raises questions concerning the personnel security fitness of an individual, the servicing security organization shall immediately assess the security factors involved and shall take suitable action to ensure that national security interests are protected. In taking such action, the security organization shall consider such factors as the conclusiveness and seriousness of the information developed, the employee's access to classified information, and the opportunity the position affords the employee to commit acts contrary to national security interests.

10-3. Under this chapter a security organization may suspend, revoke, or deny a security clearance. The FAA, FHWA, and USCG may establish their own procedures for processing adverse security actions, separate from those in this chapter, provided that they receive approval from M-40 and appropriate legal counsel, and that the procedures are consistent with the provisions of Section 5.2 of E.O. 12968. Any such procedures shall ensure that an individual whose security clearance is being denied or revoked is provided the rights and opportunities stated in Section 5.2. These opportunities include that of appearing personally and presenting relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity.

10-4. All individuals whose clearances are denied or revoked, regardless of which DOT organization takes the action, have the right to appeal the denial or revocation to the PSRB as stated in paragraphs 10-8 and 10-9.

10-5. Under the provisions of this chapter, the Secretary of Transportation may also exercise authority granted in 5 U.S.C. 7532 to suspend without pay, and then remove, a DOT employee, when the Secretary considers that action necessary in the interests of national security. The authority to remove an employee under 5 U.S.C. 7532 may not be redelegated.

Section 2 - Security Clearance Denial, Suspension, and/or Revocation

10-6. Suspension. If a decision is made to suspend a security clearance temporarily pending investigation to determine if revocation of the clearance is warranted, and the suspension exceeds 10 days, the servicing security organization shall notify the

employee in writing that it has suspended the clearance and why, to the extent consistent with the interests of national security. It shall also notify the employee's supervisor.

10-7. Post Suspension. After the security clearance is suspended, but prior to a determination on whether to reinstate or revoke it, the employee's management may, in its sole discretion: Restrict the employee to the nonsensitive duties of the position, temporarily reassign the employee to a nonsensitive position with the same grade and pay, or place the employee on administrative leave with pay. Administrative leave should be considered only if the other options are not viable.

10-8. Denial or Revocation.

a. If the security organization decides to deny or revoke a security clearance, it shall notify the individual in writing, to the extent consistent with the interests of national security, that the clearance is being denied or revoked and why. The explanation for the decision shall be as comprehensive and detailed as the national security interests of the United States and applicable laws permit. The security organization shall also notify the individual in writing that:

(1) The individual has 30 days from the date of the notification to submit a written response to the security organization with any supporting documentation; and in that response, may request the opportunity to appear personally before an adjudicative authority;

(2) The individual may request an extension of the response time, but must do so in writing to the security organization; and the granting of any extension is subject to the security organization's discretion;

(3) The individual has the right to be represented by counsel or other representative at his or her own expense and to request any documents or records of oral reports upon which the decision is based;

(4) The individual has the right to request, from the investigating agency, the entire investigative file for any investigation on which the decision is based; and

(5) If no timely response is received, the denial or revocation shall be final.

b. If the employee or applicant submits a timely response, the security organization shall consider that response and any supporting documentation timely submitted before making its final decision. If the individual asks to appear in person to respond to the denial or revocation decision, the security organization shall

provide that opportunity at Government expense. The appearance shall be before an adjudicative authority other than the investigating entity and the security organization shall allow the individual to present any documents, materials, or other information as part of the response. All such evidence shall be considered before the security organization makes its decision. The security organization shall make a written summary or recording of any such personal appearance and place it in the individual's PSF. The decision shall be in writing and, in the case of a denial or revocation, the security organization shall notify the individual that:

(1) He or she may appeal the decision to the PSRB chaired by M-40; and

(2) The review request must be in writing and must be submitted to M-40 within 30 days from the date of the decision.

c. The security organization's decision shall become the final DOT decision on the individual's security clearance if the individual does not appeal to M-40 within 30 days.

10-9. Appeal.

a. Section 5.2(a)(6) of E.O. 12968 provides each person whose security clearance has been denied or revoked an opportunity to appeal in writing to a high level panel appointed by the agency head. The Secretary has chartered the PSRB to fulfill this requirement.

b. The Board is comprised of at least three members, two of whom are selected from outside the security field.

c. The Board acts on behalf of the Secretary, except in any case in which the Secretary personally elects to make the final decision on an appeal, and makes the administratively final decision on appeals by DOT personnel, civilian or military, of security clearance denial or revocation actions originating in any DOT organization. The Board has the authority to direct the granting of a clearance that a DOT administration or organization has denied, and to direct the reinstatement of a revoked clearance as if it had never been revoked. Board decisions are in writing.

d. The Board is chaired by a member from M-40 as appointed by the Assistant Secretary for Administration (M-1) and may, with the approval of M-1, establish its own operating procedures.

e. An appeal to the Board does not stay the decision being appealed. However,

no adverse personnel action based on the denial or revocation of a clearance shall be proposed or taken against the affected person prior to the expiration of the 30-day period in which he or she may appeal the denial or revocation and until any appeal is decided by the Board.

10-10. Post Denial or Revocation.

a. After the procedures outlined in paragraphs 10-8 and 10-9 have been completed and when a security clearance has been revoked, the servicing security organization shall provide the servicing human resources organization and/or the employing organization office all information necessary to take appropriate action under applicable personnel authority and regulations. Such action may include removing the employee or permanently reassigning the employee to a nonsensitive position.

b. After the procedures outlined in paragraphs 10-8 and 10-9 have been completed and a security clearance has been denied:

1. If the individual denied a clearance is an applicant for appointment to a position for which a clearance is required, the person shall not be appointed to that position.

2. If the individual denied a clearance is an employee occupying a nonsensitive position who has been selected for a position requiring a clearance, appointment or reassignment to that position shall not be made.

Section 3 - Suspension and Removal Under Title 5 U.S.C. 7532

10-11. Under the provisions of 5 U.S.C. 7532, and additional authority as stated in E.O. 10450, Section 6, the Secretary of Transportation may suspend without pay, and then remove, a DOT employee when the Secretary considers that action necessary in the interests of national security. This action is separate and distinct from actions that DOT may take in regard to security clearance revocations as prescribed in Section 2 above, which do not require approval by the Secretary.

10-12. In lieu of suspension without pay, the Secretary may temporarily detail to a nonsensitive position an employee who occupies a sensitive position.

10-13. Whenever a servicing security organization believes that action under 5 U.S.C. 7532 is warranted, it shall provide all pertinent information, in writing, to M-40.

10-14. If after reviewing the information from the security organization the Director,

M-40, believes that either suspension or detail to a nonsensitive position is warranted, he or she shall provide all pertinent information to the Secretary and shall recommend appropriate action.

10-15. If the Secretary chooses to suspend the employee or detail him or her to a nonsensitive position, if appropriate, M-40 shall then notify the employee, to the extent that the interests of national security permit, of the reasons for the suspension or detail. Within 30 days after the notification, the employee is entitled to submit to the Director, M-40, statements or affidavits to show why he or she should be restored to duty.

10-16. After a suspension without pay or detail to a nonsensitive position, and before the Secretary removes an employee under 5 U.S.C. 7532 and E.O. 10450, and if the employee has a permanent appointment, has completed a probationary or trial period, and is a citizen of the United States, M-40 shall give the employee:

a. A written statement of charges against the employee within 30 days after the suspension or detail. The statement shall be subject to amendment within 30 days and shall be as specific as security considerations will permit. Each charge shall relate to the security standard and criteria as stated in Chapter 3, Section 2. The statement shall cite 5 U.S.C. 7532 as authority for the proposed removal action.

b. An opportunity within 30 days thereafter (plus an additional 30 days if the charges are amended) to answer the charges and submit affidavits or other material to support the employee's response. M-40 shall advise the employee that if no reply is received the case will be decided on the basis of the available information. M-40 shall also advise the employee that the purpose of the reply shall be to respond to each of the charges with any information and supporting documents that would explain, clarify, refute, or have other significant benefit in regard to the substance of the charges. In addition, M-40 shall advise the employee that he or she may request a hearing on the charges.

10-17. M-40 shall review any reply to the statement of charges and determine whether the employee has submitted additional substantive information, which justifies withdrawal of the proposed removal action.

10-18. If the employee requests a hearing on the charges, the Director, M-40, shall inform the Secretary of the need to convene a security hearing board. The Secretary may then select at least three persons to serve on the board, which shall report to the Secretary the facts of the case and a recommended decision. (These individuals shall be different persons from those who serve on the PSRB described in Section 2 above, paragraph 10-9.) M-40 shall provide administrative services to the hearing board. DOT is responsible for providing a

qualified attorney to act as counsel for the board and for providing necessary stenographic services to record proceedings.

10-19. The Secretary, or an official whom the Secretary has specifically designated, shall review the case before a decision adverse to the employee is made final. The Secretary may direct further investigation of specific matters, if warranted, and may reconvene the security hearing board to review additional information.

10-20. If the Secretary or M-40 determines that the employee should be restored to his or her position, either the Secretary, an official designated by the Secretary, or M-40 shall so notify the employee and all officials concerned. If M-40 believes that a reply from the employee does not warrant a favorable determination and if the employee has not requested a hearing, the Director, M-40, shall refer the completed case to the Secretary with a recommendation that the Secretary direct removal of the employee on the basis of the stated charges.

10-21. Either the Secretary, an official designated by the Secretary, or M-40 shall provide the employee with a written statement of the Secretary's decision and shall give copies of the statement to all officials concerned. The decision of the Secretary shall be final.

10-22. If an employee does not have a permanent or indefinite appointment, has not completed a probationary or trial period, or is not a citizen of the United States, M-40 shall give the employee 30 days after the suspension or detail to submit any statements or affidavits to M-40 as to why he or she should be reinstated in his or her position. Following M-40 review of any material that the employee submits, the Director, M-40, may recommend removal action to the Secretary. The Secretary may then remove the employee if the Secretary agrees that such action is necessary in the interests of national security. This authority to remove an employee may not be redelegated.

Section 4 - Employment of Individuals Previously Separated for Security Reasons

10-23. No person who has been separated from employment with any department or agency of the U.S. Government under any Federal security program (such as 5 U.S.C. Sections 7531-33, E.O. 9835, or E.O. 10450) may be employed in DOT without prior approval of the Secretary and determination by the servicing human resources organization that the factors leading to the separation are not currently disqualifying for DOT employment. When employment of such a person is proposed, the servicing security organization shall obtain complete information regarding the basis for the separation, ensure appropriate investigation of the person's subsequent activities, ascertain whether the human resources organization has determined that the person is eligible for DOT employment, and obtain any other information the Secretary needs to decide whether or not the person's employment is clearly consistent with the interests of national security. The security organization shall then forward this information to M-40 for forwarding to the Secretary. This approval authority may not be redelegated.

Chapter 11

FOREIGN ASSIGNMENTS AND TRAVEL

11-1. General. Special safeguards are required to protect the national interest and national security information when DOT personnel and representatives are given foreign assignments or perform official foreign travel. For this purpose, a "foreign" location means outside the 50 states, the District of Columbia, Puerto Rico, or any United States possession, territory, or trust territory. The investigative requirements and security precautions specified in this chapter apply to employees and representatives on foreign assignments or travel. DOT personnel assigned official travel in a foreign country must exercise good judgment at all times to ensure that they do nothing contrary to the interests of the United States or DOT. Officials authorizing the travel are responsible for ensuring that each traveler possesses the good character and reliability needed for the assignment.

11-2. Investigative and Clearance Requirements.

a. Foreign assignments.

(1) A DOT employee serving in a foreign duty location will normally be assigned to the U.S. diplomatic or consular mission in the country of residence. To comply with DOS regulations, all employees assigned to work in or have unescorted access to the controlled access area of an embassy or embassy annex must hold at least a Top Secret clearance. Other employees are not required to hold security clearances unless their duties will require them to have access to classified information.

(2) All foreign positions shall be designated at least critical-sensitive, and persons selected for these positions shall have at least a completed and favorably adjudicated BI prior to transfer to the foreign location.

(3) When an employee is being assigned to a foreign duty location, the servicing security organization shall transmit the security clearance data to the appropriate DOS Regional Security Officer (RSO) or Post Security Officer (PSO). The servicing security organization may do so either by electronic message directly to the RSO or PSO or by providing the data to the Bureau of Diplomatic Security, Department of State, for transmission to the post.

b. Personal service contract (PSC) personnel. U.S. citizens who are family members of U.S. personnel stationed in foreign countries, and who are technically PSC employees under arrangements made through DOS, are not required to hold security clearances if their employment will not require them to have access to classified information or to sensitive areas at locations that receive, process, or store classified or other foreign policy or operationally

sensitive information or material. A NACI is the minimum required investigation for these positions. The servicing security organization is responsible for granting any security clearances necessary for persons in these positions.

c. Temporary duty (TDY).

(1) If an employee is to be on foreign TDY intermittently or continuously for more than 120 days in one year, a completed BI is required prior to beginning the travel.

(2) For all other foreign TDY assignments, there are no special investigative requirements other than those applicable to the risk or sensitivity level of the employee's position.

(3) There is no requirement that an employee on TDY to a foreign location have a security clearance. While there is no specific clearance requirement to visit DOT offices located in foreign countries, provided access to classified information is not required, an employee requiring access to an office located in an embassy or embassy annex must be escorted if he or she does not have at least a Secret clearance.

(4) When an employee is scheduled for TDY to a foreign location, the organization where the employee works should determine whether or not a clearance will be required for the work the employee will be doing and/or to avoid major inconvenience due to lack of unescorted access to particular Government agency offices. In making this determination, the office should consider such factors as the nature of work to be performed; the extent, nature, and location of contacts with DOT and other Government officials; and the length of the TDY. In many cases, not being allowed unescorted access for one visit to an office or embassy in a foreign location will cause an employee no significant inconvenience.

(5) When an office determines that clearance information should be provided to DOS for an employee scheduled for TDY, it shall contact its servicing security organization as far in advance of the trip as possible. DOS requires that the level of clearance be stated in the travel message and on the travel authorization. However, no such information shall appear on any message or travel authorization without coordination with the security organization.

(6) If an employee scheduled for TDY needs a security clearance and does not have one, the operating office shall send a written request to the servicing security organization for a temporary clearance. The request shall

state the period of time for which the clearance is needed, the location(s) to be visited, and specifically why the clearance is necessary.

(7) Security organizations shall transmit clearance data for employees going on TDY, as necessary, as stated in paragraph a (3) above.

d. International conferences.

(1) Head of a delegation. Any DOT employee selected to head a delegation from the United States to an international conference on other than a one-time basis shall be subject to a BI.

(2) Nominee as DOT representative at an international conference. Nomination to represent DOT at an international conference is subject to completion of a NAC or higher level investigation. This investigation has normally been conducted on Federal employees, but not necessarily on technical advisors or other representatives from industry. If an advisor from industry is selected to help represent DOT at an international conference, the DOT office arranging for the advisor's services shall contact its servicing security organization at least three weeks prior to the date that the delegation is scheduled to depart. The security organization shall then determine if a NAC has already been conducted on the industry representative, as may be the case, for example, if the person holds a Government security clearance or is a military reservist. If a NAC has not been completed, the security organization shall furnish the responsible office the forms for the person to complete. The office shall then ensure that they are completed and returned to the security organization, which shall then process the NAC. A NAC for this purpose need not include a completed fingerprint check prior to the delegation's departure.

e. Special requirements. Visits to some activities at foreign locations require special security authorizations or clearances. For example, to attend a meeting at the North Atlantic Treaty Organization (NATO) headquarters in Brussels, Belgium, NATO requires a person to have a NATO clearance. An office arranging for a DOT employee to visit NATO headquarters or a similar activity shall ensure in advance that it requests its servicing security organization to process any special clearance(s) required. The office should ask about clearance requirements when making the visit arrangements and provide its request to the security organization at least 3 weeks in advance of the visit to allow time for processing.

Appendix 1

SECURITY ADJUDICATION GUIDELINES

Section 1 - General

The following adjudication guidelines, officially the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, were developed by the Security Policy Board as required by E.O. 12968. In March 1997 the President approved them for use throughout the Executive Branch. All DOT security organizations shall use these guidelines when determining whether the granting or continuation of eligibility for access to classified information is consistent with the interests of national security.

Section 2 - The Adjudicative Process

1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the "whole person" concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

    a. the nature, extent, and seriousness of the conduct;
    b. the circumstances surrounding the conduct, to include knowledgeable participation;
    c. the frequency and recency of the conduct;
    d. the individual's age and maturity at the time of the conduct;
    e. the voluntariness of participation;
    f. the presence or absence of rehabilitation and other pertinent behavioral changes;
    g. the motivation for the conduct;
    h. the potential for pressure, coercion, exploitation, or duress; and
    i. the likelihood of continuation or recurrence.

2. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether a person's access to classified information is clearly consistent with national security will be resolved in favor of the national security.

3. The ultimate determination of whether the granting or continuation of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person:

a. GUIDELINE A: Allegiance to the United States;
b. GUIDELINE B: Foreign influence;
c. GUIDELINE C: Foreign preference;
d. GUIDELINE D: Sexual behavior;
e. GUIDELINE E: Personal conduct;
f. GUIDELINE F: Financial considerations;
g. GUIDELINE G: Alcohol consumption;
h. GUIDELINE H: Drug involvement;
i. GUIDELINE I: Emotional, mental, and personality disorders;
j. GUIDELINE J: Criminal conduct;
k. GUIDELINE K: Security violations;
l. GUIDELINE L: Outside activities; and
m. GUIDELINE M: Misuse of Information Technology Systems.

4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole person concept, pursuit of further investigation may be terminated in the face of reliable, significant, and disqualifying adverse information.

5. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

   a. voluntarily reported the information;
   b. was truthful and complete in responding to questions;
   c. sought assistance and followed professional guidance, where appropriate;
   d. resolved or appears likely to resolve the security concern favorably;
   e. has demonstrated positive changes in behavior and employment;
   f. should have his or her access temporarily suspended pending final adjudication of the information.

6. If after evaluating information of security concern the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

Section 3 - Specific Guidelines

GUIDELINE A
Allegiance to the United States

The concern: An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to question an individual's allegiance to the United States.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act the aim of which is to overthrow the Government of the United States or alter the form of Government by unconstitutional means;
2. association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;
3. association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means; and
4. involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;
2. the individual's involvement was only with the lawful or humanitarian aspects of such an organization;
3. the individual's involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest; and
4. the person has had no recent involvement or association with such activities.

GUIDELINE B
Foreign Influence

The concern: A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. an immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;
2. sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;
3. relatives, cohabitants, or associates who are connected with any foreign Government;
4. failing to report, where required, associations with foreign nationals;

5. unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;
6. conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign Government;
7. indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion, or pressure; and
8. a substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. a determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;
2. contacts with foreign citizens are the result of official United States Government business;
3. contact and correspondence with foreign citizens are casual and infrequent;
4. the individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country; and
5. foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

GUIDELINE C
Foreign Preference

The concern: When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. the exercise of dual citizenship;
2. possession and/or use of a foreign passport;
3. military service or a willingness to bear arms for a foreign country;
4. accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;
5. residence in a foreign country to meet citizenship requirements;
6. using foreign citizenship to protect financial or business interests in another country;
7. seeking or holding political office in the foreign country;
8. voting in foreign elections; and
9. performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another Government in preference to the interests of the United States.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. dual citizenship is based solely on parents' citizenship or birth in a foreign country;
2. indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;
3. activity is sanctioned by the United States; and
4. the individual has expressed a willingness to renounce dual citizenship.

GUIDELINE D
Sexual Behavior

The concern: Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. (The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.) Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
2. compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;
3. sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and
4. sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;
2. the behavior was not recent and there is no evidence of subsequent conduct of a similar nature;
3. there is no other evidence of questionable judgment, irresponsibility, or emotional instability; and
4. the behavior no longer serves as a basis for coercion, exploitation, or duress.

GUIDELINE E
Personal Conduct

The concern: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in

an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

1. refusal to undergo or cooperate with required security processing, including medical and psychological testing; or
2. refusal to complete required security forms or releases, or provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying also include:

1. reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;
2. the deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
3. deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;
4. personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;
5. a pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency; and
6. association with persons involved in criminal activity.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;
2. the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;
3. the individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;
4. omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;
5. the individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;
6. a refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon

being made aware of the requirement, fully and truthfully provided the requested information; and

7. association with persons involved in criminal activities has ceased.

GUIDELINE F
Financial Considerations

The concern: An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. a history of not meeting financial obligations;
2. deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;
3. inability or unwillingness to satisfy debts;
4. unexplained affluence; and
5. financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the behavior was not recent;
2 it was an isolated incident;
3. the conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce, or separation);
4. the person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
5. the affluence resulted from a legal source; and
6. the individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

GUIDELINE G
Alcohol Consumption

The concern: Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, and failure to control impulses; and increases the risk of unauthorized disclosure of classified information due to carelessness.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;
2. alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;
3. diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;
4. evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;
5. habitual or binge consumption of alcohol to the point of impaired judgment; and
6. consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the alcohol-related incidents do not indicate a pattern;
2. the problem occurred a number of years ago and there is no indication of a recent problem;
3. positive changes in behavior supportive of sobriety; and
4. following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

GUIDELINE H
Drug Involvement

The concern:

1. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

2. Drugs are defined as mood and behavior altering substances, and include:

   (a) drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

   (b) inhalants and other similar substances.

3. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. any drug abuse (see above definition);
2. illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;
3. diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;
4. evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program; and
5. failure to complete successfully a drug treatment program prescribed by a credentialed medical professional. Current drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the drug involvement was not recent;
2. the drug involvement was an isolated or infrequent event;
3. a demonstrated intent not to abuse any drugs in the future; and
4. satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.

GUIDELINE I
Emotional, Mental, and Personality Disorders

The concern: Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social, and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. When appropriate, a credentialed mental health professional (e.g., clinical psychologist or psychiatrist), acceptable to or approved by the Government, should be consulted so that potentially disqualifying and mitigating information may be fully and properly evaluated.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. an opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;
2. information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;
3. a pattern of high-risk, irresponsible, aggressive, anti-social, or emotionally unstable behavior; and
4. information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. there is no indication of a current problem;
2. recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured or in remission and has a low probability of recurrence or exacerbation;
3. the past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

GUIDELINE J
Criminal Conduct

The concern: A history or pattern of criminal activity creates doubt about a person's judgment, reliability, and trustworthiness.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. any criminal conduct, regardless of whether the person was formally charged and
2. a single serious crime or multiple lesser offenses.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the criminal behavior was not recent;
2. the crime was an isolated incident;
3. the person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;
4. the person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur; and
5. there is clear evidence of successful rehabilitation.

GUIDELINE K
Security Violations

The concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. unauthorized disclosure of classified information; and
2. violations that are deliberate or multiple or due to negligence.

Possible mitigating conditions: Conditions that could mitigate security concerns include actions that:

1. were inadvertent;
2. were isolated or infrequent;
3. were due to improper or inadequate training; and/or
4. demonstrate a positive attitude toward the discharge of security responsibilities.

GUIDELINE L
Outside Activities

The concern: Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:

1. a foreign country;
2. any foreign national;
3. a representative of any foreign interest; and/or
4. any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities; and
2. the individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

GUIDELINE M
Misuse of Information Technology Systems

The concern: Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to protect properly classified systems, networks, and information. Information technology systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Possible disqualifying conditions: Conditions that could raise a security concern and may be disqualifying include:

1. illegal or unauthorized entry into any information technology system;
2. illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;
3. removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations; and
4. introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations.

Possible mitigating conditions: Conditions that could mitigate security concerns include:

1. the misuse was not recent or significant;
2. the conduct was unintentional or inadvertent;
3. the introduction or removal of media was authorized;
4. the misuse was an isolated event; and
5. the misuse was followed by a prompt, good faith effort to correct the situation.

Appendix 2

INVESTIGATING CONTRACTOR EMPLOYEES

1. General. This appendix states policy and procedures for the personnel security program as it relates to DOT contractor employees. It applies to contractor employees who have access to DOT facilities, sensitive information, and/or resources; and to other persons who have such access by agreement of a DOT organization.

2. Background. Many contractor employees are part of the DOT work force or closely support the DOT missions. Because of their DOT identification, the extent of their responsibility, and the risk levels of the positions they occupy, DOT investigates certain contractor employees to determine their suitability for access to DOT facilities, sensitive information, or resources.

3. Authority to investigate contractor employees.

a. The Department of Justice (DOJ) rendered an opinion October 1, 1979, that Federal agencies have the authority to screen contractor employees in any reasonable manner and that such screening must be consistent with due process of law. DOJ cited from the United States Code (U.S.C.) three statutory sources of agency authority to investigate and determine the suitability of contractor employees. These authorities are:

(1) 5 U.S.C. 301. Authorizes the head of each executive or military department to "prescribe regulations for the Government of [the] department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property."

(2) 44 U.S.C. 3102. Requires each Federal agency to provide for "effective controls over the creation and over the maintenance and use of records in the conduct of current business" and in cooperation with the Administrator of GSA to "promote the maintenance and security of records deemed appropriate for preservation."

(3) 5 U.S.C. 552a(e)(9) and (10). Requires that each agency establish: (1) Rules of conduct for persons involved in the design, operation, or maintenance of any Privacy Act system of records; and (2) appropriate administrative, technical; and physical safeguards to ensure the security and confidentiality of Privacy Act records. DOJ noted that U.S.C. 552a, while applicable only to Privacy Act systems of records, does provide that agencies, consistent with their authority, shall extend the requirements of the section to Government contractors who operate such a system of records to accomplish agency functions.

b. OMB Circular A-130, Management of Federal Information Resources, requires Federal agencies to establish personnel security policies for Federal and contractor personnel as needed to ensure an adequate level of security for Federal automated information systems. These policies should include requirements for screening all individuals participating

in the design, development, operation, or maintenance of sensitive applications, as well as those persons having access to sensitive data.

4. Definition of sensitive information. P.L. 100-235, the Computer Security Act of 1987, defines sensitive information as any information which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, USC (the Privacy Act), but that has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive data at DOT also include proprietary data.

5. Policy.

a. Except as stated in this appendix, the personnel security program requirements and procedures applicable to DOT employees shall also apply to contractor employees who have comparable access to the agency's facilities, sensitive information, or monetary or material resources. In addition, these requirements and procedures, and the specific requirements regarding contractor employees as stated in this appendix, also apply to other persons who have such access by virtue of an agreement between a DOT organization and another party. No contractor employee or applicant for contractor employment shall be prevented from having access to DOT facilities, sensitive information, or resources because of information revealed in a background investigation unless DOT has given that person an opportunity to respond to any information used as a basis to deny such access. The servicing security organization, after coordination and consultation with the contracting office, is responsible for adjudicating the suitability of contractor employees.

b. Contracts requiring contractor employees to have access to classified information shall be prepared and processed according to the procedures of the NISP as specified in Appendix 3.

6. Responsibilities.

a. DOT organizations shall:

(1) Ensure that all proposed solicitations and contracts are reviewed to determine whether or not contractors or contractor employees will have access to DOT facilities, sensitive information or resources. When they will have such access, the organization shall ensure coordination with the servicing security organization prior to issuance of the solicitation to determine any applicable personnel security investigative requirements. These requirements also apply to any proposed agreements with outside parties, other than contractors, that would result in non-DOT personnel having such access.

(2) Ensure that whenever a solicitation, contract, or agreement requires investigation of any contractor employees, the document contains language sufficient to achieve this objective in an orderly and expeditious manner. The document shall also contain language allowing DOT to deny a contractor employee or other person access to DOT facilities, information, and/or resources if the servicing security organization determines that that person is unsuitable.

(3) Ensure that the servicing security organization is notified whenever there is a change in the status of an existing contract where contractor employees are subject to investigation (i.e., replaced, defaulted, terminated, etc.).

(4) Ensure that contractors submit for their employees (including prospective contractor employees) to the servicing security organization completed forms and information for each person subject to investigation as required by the applicable contract.

(5) Ensure that a contractor employee is not allowed to work in a high or moderate risk position unless the servicing security organization has received all forms necessary to conduct any required investigation and has given its approval.

(6) Ensure that the servicing security organization is notified of any information it receives that raises a question about the suitability of a contractor employee.

(7) Ensure that any appropriate action the servicing security organization directs is taken whenever a question has arisen regarding the suitability of a contractor employee. Appropriate action may include temporarily denying the contractor employee access to DOT facilities, sensitive information, and/or resources pending resolution of an issue raising a question of suitability.

(8) Ensure that appropriate action is taken when the servicing security organization determines that a contractor employee is unsuitable for access to DOT facilities, sensitive information, and/or resources. Appropriate action may include excluding the contractor employee from working on any aspect of the DOT contract.

(9) Ensure that the servicing security organization is notified whenever a contractor employee has completed work under the contract or leaves his or her position with the contractor.

b. Servicing security organizations shall:

(1) Determine, in consultation with contracting officers, which contracts require personnel security investigation of the contractor and/or contractor employees.

(2) Determine the types of investigation to be conducted on specific contractor employees.

(3) Assist contracting officers in developing appropriate language for inclusion in solicitations, contracts, and agreements.

(4) Receive and process forms to initiate required investigations on contractor employees.

(5) Adjudicate the results of personnel security investigations of contractor employees and determine suitability in consultation with contracting officer, contracting officers' technical representatives , and other offices on a need-to-know basis.

(6) Conduct or arrange for additional investigation when necessary to resolve suitability issues.

(7) Provide contractor employees an opportunity to respond to information developed during an investigation prior to taking any unfavorable action based on that information.

(8) Notify the contracting officer in writing of any contractor employee found unsuitable for access to DOT facilities, sensitive information, and/or resources and direct action to deny such access.

(9) Direct appropriate action to be taken whenever any information is received that raises a question about a contractor employee's suitability.

(10) Maintain records on contractor employee personnel security investigations and maintain personnel security files, as necessary, on contractor employees.

(11) Provide the contracting officer with all DOT security directives that the contractor needs to fulfill security responsibilities under the contract.

7. Designating position risk levels.

a. Contractor employee positions shall be designated as either high risk, moderate risk, or low risk. The servicing security organization may do the designations or may defer to the organization for which the contract is let to make these determinations. In any event, the security organization shall have final approval authority over all designations. In general, the policies specified in Chapter 4 shall apply in designating positions in terms of suitability and AIS. However, there is no requirement to use any particular designating system. The designating organization may use the risk level designation process outlined in Chapter 4, Section 2, to help ensure uniformity and consistency in these designations. The organization shall also maintain documentation as to how the risk levels of contractor employee positions were determined.

b. Contractor employee positions may be designated in groups or by category rather than by individual position.

8. Investigative requirements for contractor employees.

a. Except as provided below, contractor employees having comparable exposure to DOT facilities, sensitive information, and/or resources shall be subject to the same investigative requirements, based on the risk level of their positions, as DOT employees.

b. Specific requirements and exceptions are as follows:

(1) High risk positions. All contractor employees in these positions shall be subject to a BI. Whenever possible, this investigation should be completed and favorably adjudicated before the employee is allowed to perform the position's duties. However, the servicing security organization may grant approval for the employee to begin work earlier, provided that it has considered the nature of the DOT facilities, sensitive information, and resources to which the employee will have access. In giving this approval, the security organization may also limit the facilities, information, and/or resources to which the employee has access pending completion of the investigation. If the BI cannot be completed before the employee must begin work on the DOT contract, the servicing security organization shall make every effort to complete at least a check of the person's fingerprints with the FBI Identification Division, or an appropriate law enforcement agency check, as soon as possible. At a minimum, a contractor employee may not perform the duties of a high risk position until all necessary investigative forms have been submitted to the servicing security organization. Except as stated in this paragraph, the specific investigative requirements for high risk positions stated in paragraph 5-12 of this order also apply to contractor employees.

(2) Moderate risk positions. All contractor employees in these positions shall be subject to at least a NACI investigation. In addition, those employees in positions with significant fiduciary responsibilities, as determined by the servicing security organization, shall be subject to a credit check. Whenever possible, the investigation shall be completed and favorably adjudicated before the employee is allowed to perform the position's duties. However, the security organization may grant approval for the employee to begin work earlier, provided that it has considered the nature of the DOT facilities, sensitive information, and resources to which the employee will have access. In giving this approval, the security organization may also limit the facilities, information, and/or resources to which the employee has access pending completion of the investigation. If the investigation cannot be completed before the employee must begin work on the DOT contract, the security organization shall make every effort to complete at least a fingerprint or appropriate law enforcement agency check as soon as possible; and, in the case of a position with significant fiduciary responsibilities, a credit check. At a minimum, a contractor employee may not perform the duties of a moderate risk position until all necessary investigative forms have been submitted to the security organization. Except as stated in this paragraph, the specific investigative requirements for moderate risk positions stated in paragraph 5-13 of this order also apply to contractor employees.

(3) Low risk positions. Except as specified below, the minimum investigative requirement for contractor employees in these positions is a fingerprint check. Depending on the extent of access to DOT facilities, sensitive information, or resources, the servicing

security organization may require a more extensive investigation, up to and including an NACI. The security organization, after consultation with the contracting office, may require submission of all required forms before the employee can receive the access.

(4) Temporary positions. Contractor employees in low risk positions that are intermittent, seasonal, per diem, or temporary and who do not work on the DOT contract in excess of 180 days in either a single assignment or a series of assignments are exempt from any investigative requirement. This exemption does not preclude investigating the person under the normal investigative requirements.

(5) Construction workers. Investigative requirements for construction workers will vary depending on the location and type of construction. In determining whether or not to conduct any investigation of these persons, the servicing security organization should consider those factors and the extent of the contractor employees' access, particularly unescorted access, to DOT facilities, sensitive information, and resources. Many of these employees will be exempt as temporary personnel. However, longer-term construction personnel with such access shall have, at a minimum, a fingerprint check.

(6) Delivery personnel and repair technicians. These contractor employees are exempt from any investigative requirement even if they are working under a DOT contract for an extended period of time. However, depending on the extent of their access at a facility, they may require an escort if they have not been investigated.

(7) Contractor personnel requiring access to classified information. When contractor employees require access to classified information and DOD investigates them under the NISP, as stated in Appendix 3, the servicing security organization is not required to initiate any additional investigation.

c. The provisions of Chapter 6, Reciprocity and Standards for Using Previous Investigations, also apply to contractor employees.

9. Initiating investigations.

a. The contracting officer has the primary responsibility for ensuring that required, completed forms for investigation of contractor employees are submitted to the servicing security organization prior to the employees receiving access to the facilities, information, or resources that make them subject to investigation. The office for which the contracted work is being done shall assist the contracting officer as necessary.

b. Specific forms are required to initiate investigations for low, moderate, and high risk positions:

(1) For low risk positions requiring only a fingerprint check, the contractor employee shall be required to submit an FD-258, FBI Fingerprint Chart. For any low risk position, however, the servicing security organization may also require submission of SF 85P, Questionnaire for Public Trust Positions, or SF 85, Questionnaire for Nonsensitive Positions. One of these forms is required to conduct a NAC or NACI.

(2) For moderate and high risk positions, the contractor employee shall be required to submit the FD-258 and an SF 85P.

(3) For any contractor employee position, the servicing security organization may also require submission of OF 306, Declaration for Federal Employment, or other form needed to comply with OPM requirements.

c. Because of the sensitive nature of the forms required for investigations, and because of Privacy Act requirements, the servicing security organization and the contracting officer should establish procedures for contractor employees to submit the forms directly to the security organization or to the contracting officer for forwarding to the security organization. These procedures shall ensure that an employee submits the forms directly to DOT in a sealed envelope and that neither the employee's supervisor nor other company personnel have access to them.

d. When initiating only a fingerprint check, the servicing security organization may do so directly with the FBI or, by appropriate agreement, through OPM.

e. When initiating an NACI or higher level investigation, the servicing security organization may do so through any Government agency, including any organization within DOT, that provides this service.

f. Each DOT organization shall establish procedures to pay for investigations on contractor employees.

10. Adjudicating investigations.

a. The servicing security organization shall adjudicate all reports of investigation on contractor employees to determine their suitability. In those cases where the security organization believes that information developed during the course of an investigation might result in an unfavorable suitability determination, it shall consult with the contracting officer.

b. In adjudicating contractor employee investigations, the servicing security organization shall apply the same suitability standard and criteria used in adjudicating investigations on competitive service applicants and employees, as stated in 5 CFR Part 731. FAA may apply the suitability standards in use for its own applicants and employees.

c. Before DOT denies a contractor employee access to its facilities, sensitive information, or resources because of information received as the result of investigation, the servicing security organization shall provide the employee an opportunity to respond to the

information. The primary purpose of this requirement is to avoid, to the extent possible, instances where DOT makes a decision adverse to an individual and possibly affecting contract performance based on erroneous information and/or mistaken identity. The security organization may provide this opportunity either orally during an interview with the contractor employee, or in writing. In either case, the security organization shall clearly explain the unfavorable information and provide the employee the opportunity to respond. It shall then consider any information the employee has provided before making a final suitability determination. DOT does not have to give the employee any additional opportunity to respond to the decision. This determination by the security organization is independent of any additional qualification determinations that are to be made by the contracting officer pursuant to contract provisions.

d. When providing a contractor employee the opportunity to respond to information and when adjudicating investigative results, the servicing security organization shall communicate with an employee directly rather than through a supervisor or other contractor official. No DOT employee shall disclose to a contractor information contained in an investigation on a contractor employee or the specific reason(s) for any suitability determination. Contracting officers shall ensure that contractors understand these procedures and the reasons for them.

e. In the case of an unfavorable suitability determination, the servicing security organization shall notify the contracting officer in writing. The contracting officer shall then notify the contractor to remove the employee as otherwise objectionable from performance under the contract, or to take other action as the security organization directs. For example, the security organization may deny the person access to DOT facilities but may still allow him or her to work on the DOT contract at another location.

11. Foreign nationals as contractor employees. In general, foreign nationals may work as DOT contractor employees on unclassified contracts and may have access to DOT facilities, information, and resources under other agreements to which DOT is a party. In any situation where the DOT organization for which the contracted work is to be done and/or the servicing security organization determine that it is in DOT's best interest to restrict access or work on a contract to United States citizens only, the appropriate contract or other agreement shall specify that restriction. In determining whether or not to apply this restriction in a given situation, DOT personnel shall consider the nature and extent of access, particularly in regard to sensitive or proprietary information. They should also ensure appropriate legal review of any contract clause applying this restriction.

12. Records on contractor employees.

a. The servicing security organization shall maintain a record of each investigation of any kind conducted on a contractor employee. The security organization may also maintain PSF on contractor employees when there are reports of investigation or other records warranting retention. These records shall be maintained for as long as the employees are working on a DOT contract. After that time, the security organization shall maintain them for the same lengths of time as for separated DOT employees.

These records will serve as the primary means by which any servicing security organization can determine if a particular contractor employee has been investigated, which is especially important if the employee is assigned to work at DOT in the future or applies for DOT employment.

b. Personnel security records contain sensitive, highly privileged, and, in some cases, classified information. All DOT personnel shall carefully protect these records in their handling, transmittal, storage, and release. The provisions of Chapter 2, Section 2, of this order also apply to personnel security records on contractor employees.

c. Upon request, a servicing security organization shall provide a contractor employee the opportunity to review any file on him or her that the security organization maintains. The employee may also, in writing, authorize a representative to review it. When complying with a request for a file review, the security organization shall follow the same policies as those used in processing Privacy Act requests for files on DOT employees, as specified in Chapter 2, Section 3.

Appendix 3

NATIONAL INDUSTRIAL SECURITY PROGRAM

1. General. This appendix states policy and procedures for implementing the NISP at DOT. It implements E.O.12829, NISP; and the industrial security policies contained in the latest edition of DOT Order 1640.4, Classified Information Management. These policies and procedures apply whenever contractors, contractor employees, subcontractors, consultants, or other persons (hereafter referred to as contractor employees) performing work for or under the direction of a DOT administration or organization require access to classified information in order to perform their duties.

2. Background.

   a. E.O. 12829 established the NISP on January 6, 1993. The National Security Council is responsible for providing overall policy direction for the NISP and the President has designated the Secretary of Defense as the NISP Executive Agent. The Director, Information Security Oversight Office is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies. By agreement between DOT and DOD, DOT authorizes DOD to act for and on behalf of DOT in providing security services for the protection of classified information that DOT releases to contractors, contractor employees, and consultants.

   b. When acting as a contracting agency, DOT has the authority and responsibility and performs the functions specified for a user agency in the latest editions of the National Industrial Security Operating Manual (NISPOM) and the Industrial Security Regulation (ISR), both of which are issued by DOD. DOD grants facility clearances to contractors as needed and grants security clearances to contractor employees when necessary for access to classified information.

3. Classified contract processing procedures.

   a. Whenever a proposed contract, as defined in Chapter 1, Section 4, would require persons not employed by the U.S. Government to have access to classified information, the office for which the work is to be done (operating office) shall include that information in a statement with the procurement request. The office shall also prepare and submit with the request a draft DD Form 254, Contract Security Classification Specification. The DD 254 shall be prepared as specified in the ISR or other DOD regulations or instructions. The office shall coordinate the draft DD 254 with its servicing security organization to ensure appropriate classification.

   b. The contracting office shall review all proposed procurement actions to determine if DOT will need to share classified information with a contractor

during precontract negotiations. If that is the case, the contracting office shall advise the security organization and provide it with a list of prospective bidders. The contracting office shall coordinate with the appropriate DSS office to determine if any prospective bidders require processing for a facility security clearance in accordance with the NISPOM, ISR, and/or other DOD regulations. The contracting office is responsible for taking action required by DOD shall issue a DD 254, signed by the contracting officer, for each request for proposal, invitation for bid, request for quotation, or other solicitation.

c. The contracting office shall issue a completed DD 254 with the award of each classified contract, including follow-on contracts, and shall provide a copy of the form to its servicing security organization.

d. Each classified contract or consulting agreement shall contain a security clause specifying everything that a contractor, contractor employee, or consultant has to do to ensure that the DOT organization and DSS can process all contractors and individuals for any needed facility or security clearances, and do so according to requirements and procedures stated in the NISPOM, ISR, or other DOD regulations. The contract shall also specify that requests for classified visits shall be in accordance with the NISPOM and shall be certified by the contracting office prior to forwarding to the organization to be visited.

e. DSS will work directly with contractors, contractor employees, and consultants to grant facility clearances and to grant security clearances to individuals.

f. The contracting office shall notify the security organization and DSS whenever the status of a contract changes (i.e., replaced, defaulted, or terminated).

4. Annual review of DD 254. Annually on the anniversary date of the contract, or more often if required by the ISR or other DOD regulation, the operating office shall review the DD 254 for accuracy and currency. If changes are necessary, the operating office and the contracting office, in coordination with the servicing security organization, shall issue a revised DD 254, preparing it as specified in the ISR or other DOD regulation. If no change is necessary, the operating office shall notify all holders of the DD 254 that it is current in all respects.

5. Visit requests. Whenever a contractor employee or consultant is required to visit a DOT facility and will be required to have access to classified information, the contracting office shall complete, certify, and process a visit request as specified in the NISPOM, ISR, or other DOD regulation. The contracting office shall provide an information copy of a certified visit request to the security organization for the facility to be visited.

Appendix 4

INVESTIGATING CHILD CARE SERVICES WORKERS

1. General. This appendix states policy and procedures for the personnel security program as it relates to suitability checks on child care services workers. It applies to persons working in DOT-sponsored child care services facilities as either employees or volunteers.

2. Background.

   a. 42 U.S.C. Section 13041 (originally Subtitle E of the Crime Control Act of 1990, Public Law 101-647), requires criminal history background checks on child care services employees either hired by or under contract to the Federal Government. In accordance with General Services Administration (GSA) guidelines, the DOT Child Care Handbook also states that suitability checks shall be conducted on all child care center employees and shall include criminal records and background checks.

   b. 42 U.S.C. 13041 defines "child care services" as including, but not limited to, child (day) care, recreational programs, health and mental health care, social services, education, foster care, residential care, treatment services, and child protective services. The provisions of this law apply to services that an agency provides to children under the age of 18.

3. Policy and Procedures.

   a. Any person working in a DOT-sponsored child care services center or who provides child care services to persons under the age of 18 as part of any DOT-sponsored activity shall be subject to the requirements of this appendix. They apply to DOT employees, DOT contractor employees, DOT military personnel, and employees of DOT employee organizations or other entities providing child care services as part of a DOT-sponsored activity or by agreement with DOT to provide the services on DOT property.

   b. The requirements of this appendix do not apply when a DOT organization is participating with other Federal agencies in the joint operation of a child care services facility or when a child care services activity is on GSA controlled or leased property and another agency such as GSA is responsible for ensuring that background investigations are conducted as needed to comply with 42 U.S.C. 13041.

   c. DOT officials responsible for overseeing child care services activities or who serve as liaison with entities providing these services shall coordinate with their servicing security organization to ensure that before an applicant

is allowed to work in the activity providing these services, either as an employee or as a volunteer, he or she completes and submits to the security organization SF 85P, Questionnaire for Public Trust Positions, and the fingerprint card appropriate for the person's status. If the applicant is or will be a Federal employee, the card is the SF 87. For other persons, Form FD-258 is the appropriate card.

d. Upon receipt of the SF-85P, a security specialist trained to conduct personnel security interviews shall review the form and either interview or correspond with the applicant. Either in an interview or by correspondence, the specialist shall ask the applicant if he or she has ever been arrested for or charged with a sex crime, an offense involving a child victim, or a drug felony. 42 U.S.C. 13041(c) states, in part, that a conviction for any of these offenses may be grounds for denying employment or for dismissal of an employee from a child care services position.

e. If the SF-85P shows that a personnel security investigation has been completed within the past five years, the security organization shall attempt to obtain the results of that investigation, and, as applicable, shall apply the provisions of Chapter 6 in regard to using a previous investigation.

f. Whenever the interview, correspondence, or review of the SF-85P reveals derogatory information, the security organization shall inform the appropriate DOT official supervising or overseeing the activity that the applicant may not begin working in the facility until the appropriate investigation has been completed and favorably adjudicated. Derogatory information in this instance means an arrest for one of the offenses specified in paragraph d or other unfavorable information raising a significant issue which may eventually result in the DOT organization directing that the applicant may not work in the position providing child care services.

g. If the interview or correspondence and review of the SF-85P reveal no derogatory information, the security organization shall notify the appropriate DOT official that the applicant may begin working in the child care services activity, under supervision, pending completion of the required investigation. The person supervising the child care center or other activity shall ensure that until the investigation has been completed and favorably adjudicated, the individual is not left alone at the activity with persons under the age of 18.

h. For DOT employees and contractor employees, 42 U.S.C. 13041 requires investigation that includes a fingerprint check conducted through the FBI and criminal history records checks at the repositories for this information

in those states where the employee has listed current and former residences. The Child Care National Agency Check and Inquiries (CNACI) conducted by OPM is sufficient to meet this requirement, but the servicing security organization may conduct the investigation by any means that will result in completion of the required checks.

i. For individuals who are subject to the requirements of this appendix but who are neither DOT employees nor contractor employees, a fingerprint check is the minimum investigation required. DOT organizations may also choose to conduct a higher-level investigation.

j. DOT organizations responsible for or overseeing the provision of child care services shall establish procedures to pay for investigations on child care services workers.

k. Results of all investigations will be returned to the servicing security organization. Any unfavorable information that an investigation reveals shall be adjudicated by a DOT employee trained to adjudicate suitability investigations. The servicing human resources organization is responsible for suitability adjudications on all DOT civilian employees. For persons who are not DOT civilian employees, security organizations shall be responsible for the adjudications unless, with security organization approval, a DOT organization elects to assign that responsibility to a qualified adjudicator outside of the security organization.

l. In adjudicating investigations on child care services workers, adjudicators should generally apply the same standard and criteria in effect for investigations on Federal employees. The adjudicator shall assess all information of record, both favorable and unfavorable, for its relevance, recentness, and seriousness. Adjudicators shall provide fair, impartial, and equitable treatment for all child care services workers.

(1) Of particular concern in adjudications is any conduct or pattern of behavior indicating that a person's employment or volunteer work providing child care services might place children in jeopardy.

(2) Examples of specific conduct, actions, or convictions that shall be considered as a basis for an unfavorable suitability determination include, but are not limited to, convincing evidence, with or without a conviction, of the crime of child molestation or abuse or neglect of a child or other dependent person entrusted to the person's care; negligence that has resulted in death or serious injury to a child or other dependent person; and a pattern of arrests or evidence of a single serious

crime which raises questions about a person's suitability for the position.

(3) Of concern also is any action or pattern of behavior that might lessen the confidence of DOT personnel that an activity providing child care services is a safe, secure place for the care of their children.

m. Before the security organization or other adjudicator makes any unfavorable suitability determination, the security organization shall provide the applicant or employee an opportunity to respond to all information being considered as the basis for prohibiting the person from working at a DOT activity providing child care services. A DOT employee trained to conduct personnel security interviews shall interview the person, clearly explain the unfavorable information, and provide the individual the response opportunity. The interviewer shall also document the interview, including the information provided to the individual and the individual's response. The adjudicator shall then consider any information the applicant or employee has provided before making a final suitability determination.

n. The security organization, human resources organization, or other adjudicator shall notify the DOT official responsible for overseeing the child care services activity of the suitability determination. In the event of an unfavorable determination, this notification shall be in writing. If the individual who is the subject of the unfavorable suitability determination works as an employee or as a volunteer for a private entity, such as a child care provider or recreation association, the DOT official shall inform in writing the appropriate management official of the private entity that the individual may not work with persons under the age of 18 in a DOT-sponsored child care services activity.

o. When providing due process and adjudicating investigative results, the security organization or other adjudicator shall communicate with the individual employee or volunteer directly or through DOT personnel who have official responsibility for overseeing the child care services activity. No DOT employee shall disclose to a private contractor or to an official of a private entity the specific reason(s) for any suitability determination. DOT personnel responsible for overseeing private contractors, organizations, or other entities providing child care services shall ensure that these entities understand these procedures and the reasons for them.

p. DOT personnel responsible for arrangements for, oversight of, and liaison with employee organizations and non-DOT entities providing child care services shall make sure that all agreements with these organizations, such as agreements for use of DOT space for child care services, include

adequate provisions and language to ensure compliance with the policies and procedures stated in this appendix.

q. All DOT employees are responsible for referring to the servicing security organization any information about a person providing child care services as part of a DOT-sponsored activity that would raise a question about that person's suitability to continue to work with persons under the age of 18.

Appendix 5

POSITION RISK LEVEL DESIGNATION PROCESS

1. This appendix describes one process that DOT organizations may use to make initial risk level designations as stated in Chapter 4, Section 2. OPM developed this process for use by all Government agencies. Using it helps to ensure consistency in position risk level designations and uniformity in designations among positions with similar duties and responsibilities. Once a risk level is determined using these procedures, the designation is always subject to adjustment or change because of uniqueness, the need for uniformity, special responsibilities, the need for access to classified information, or access to automated information systems, as stated in Chapter 4, Section 2.

2. This process consists of designating each agency program for its impact and scope as related to the efficiency of the service (program placement) and then designating each position for its degree of risk to its program (tentative risk level).

3. Procedures for determining program placement are as follows:

    a. Determine the program's impact on the efficiency of the service by identifying the area of primary program focus and then relating that area to one of the impact descriptions (major, substantial, moderate, or limited) listed in the left column of Chart A. The area of primary focus should be one of the following:

        (1) Accounting for, auditing, or disbursement of public funds;

        (2) Administrative, regulatory, or policy control over public and/or private programs or operations;

        (3) Protection of national security;

        (4) Enforcement of Federal laws; or

        (5) Protection of life or property.

    b. If a program has more than one area of primary focus, or if questions arise as to placement of a program at one or two impact descriptions, base a decision on the best interests of the organization's mission.

    c. Determine the program's scope of operations in terms of the efficiency of the service, choosing from one of the scopes (worldwide, Government-wide, multi-agency, or agency) listed across the top of Chart A.

    d. Use Chart A to determine program placement (major, substantial, moderate, or limited).

4. In determining position risk points, the position's duties and responsibilities shall be

considered in the context of the program and the risk the position has for damage or abuse to the program. The procedure requires a determination of the degree of impact on the program of each of five risk factors and the assignment of points to each risk factor. The sum of the risk points and the program placement combine to determine the tentative risk level. Specific procedures are as follows:

a. Determine the degrees of impact for each of the five risk factor descriptions shown across the top of Chart B. For all of the factors except supervision received, use the degree descriptions shown in the left column. For supervision received, use the degree descriptions shown in the right column.

b. Assign a point value for each risk factor to numerically reflect the degree of impact. The greater the impact, the more points assigned. Although Chart B only shows point values of 1, 3, 5, and 7, points may be assigned at the 2, 4, and 6 values to reflect borderline determinations.

c. Add the point values for each of the risk factors to determine the total risk points.

d. Use Chart C to find the tentative risk level, applying the program placement determined above (left column) and the total risk points (top of the chart).

5. DOT Form 1630.2, Position Risk/Sensitivity Level Designation Record, may be used to record the specific steps in the designation process as outlined in this appendix, in conjunction with the procedures in Chapter 4, Section 2.

CHART A

IMPACT DESCRIPTIONS	Scope of Operations			
	WORLDWIDE: Operational activity is carried out worldwide, with primary focus in either the public or the private sector.	GOVERNMENTWIDE Operational activity is carried out Governmentwide, to all sectors, with primary focus on the public sector Governmentwide.	MULTI-AGENCY: Nationally or regionally with primary focus extending to more than one agency in the public sector, or to the elements in the private sector impacted by the agencies.	AGENCY: Operations of the agency, or an agency's region or area, with primary focus extending to the elements in the private sector impacted by the agency.
MAJOR: Impacts directly on the survival, stability, and continued effectiveness of Government operations, the promotion of major Government fiscal goals, or a primary social, political, or economic interest of the Nation.	MAJOR	MAJOR	SUBSTANTIAL	MODERATE
SUBSTANTIAL: Impacts directly on the efficiency and effectiveness of a sizeable segment of the Federal work force, or the interests of large numbers of individuals in the private sector.	MAJOR	SUBSTANTIAL	SUBSTANTIAL	MODERATE
MODERATE: Impacts directly on the effectiveness of an agency's operations, the fiscal interests of an agency, or affects the social, political, or economic interests of individuals, businesses, or organizations in the private sector.	SUBSTANTIAL	MODERATE	MODERATE	LIMITED
LIMITED: Limited impact on the operational effectiveness of one or a few programs in an agency, or the interests of a limited number of individuals in the private sector.	MODERATE	MODERATE	LIMITED	LIMITED
	PROGRAM PLACEMENT			

CHART B

RISK FACTOR DESCRIPTIONS

DEGREE OF IMPACT	DEGREE OF PUBLIC TRUST: The consensus of confident expectation for honesty, integrity, reliability, responsibility, or justice placed in a position.	FIDUCIARY MONETARY RESPONSIBILITY: Authority or ability to obligate, control, or expend public money or items of monetary (bonds, etc.) value.	IMPORTANCE TO PROGRAM: Impact the individual position has, due to status, in or influence on the program as a whole, either individually or collectively.	PROGRAM AUTHORITY: Ability to manipulate authority or control the outcome or results of all or key portions of a program or policy.	SUPERVISION RECEIVED: Frequency work is reviewed and nature of the review. **DEGREE**
MAJOR: Potential for Independently compromising the integrity and effectiveness of a major program element or component, or in conjunction with others, damaging all phases of program operations.	7	7	7	7	Limited: Occasional review only with respect to major policy issues by superior without expertise in the technical aspects of program policy and operations. 7 Points
SUBSTANTIAL: Potential for reducing the efficiency of overall program operations, or the overall operations of major program elements or components independently, or through collective action with others.	5	5	5	5	Periodic: Ongoing spot review of policy and major operational considerations of work by superior, with some knowledge of program operations, but with minimal technical program expertise. 5 Points
MODERATE: Potential for reducing the efficiency of the overall or day-to-day operations of a major program element or component, through independent action or collectively with others.	3	3	3	3	Moderate: Technical: Ongoing spot review of work in connection with important operation issues by superior with technical program expertise. 3 Points

LIMITED: Potential for damage not meeting above criteria.	1	1	1	1	Close Technical: Continuing review of all phrases of work by supervisor with technical program expertise.

POSITION RISK POINTS

CHART C

II. POSITION RISK POINTS

PROGRAM PLACEMENT	5-10	11-17	18-23	24-29	30-33	34-36
MAJOR	Low Risk	Moderate	Moderate	High Risk	High Risk	High Risk
SUBSTANTIAL	Low Risk	Moderate Risk	Moderate Risk	Moderate Risk	High Risk	High Risk
MODERATE	Low Risk	Low Risk	Moderate Risk	Moderate Risk	Moderate Risk	High Risk
LIMITED	Low Risk	Low Risk	Low Risk	Low Risk	Moderate Risk	High Risk

U.S. Department of Transportation

POSITION RISK / SENSITIVITY LEVEL DESIGNATION RECORD

FAA EMPLOYEE IDENTIFICATION

Office/Division / Branch	Organization Code or Cost Center
Position Title	Position Description Number

If the position is an national security position (security clearance required) Sections I, II and III are optional

RISK DESIGNATION SYSTEM

I. Program Placement

Impact on efficiency of service	Major ☐	Substantial ☐	Moderate ☐	Limited ☐
Scope of Operations for efficiency of service	World Wide ☐	Gov't Wide ☐	Multi-Agency ☐	Agency ☐
Placement	Major ☐	Substantial ☐	Moderate ☐	Limited ☐

II. Position Risk Points

a. Degree of public trust	(7-1) ----------	_____
b. Fiduciary responsibilities	(7-1) ----------	_____
c. Importance to program	(7-1) ----------	_____
d. Program authority level	(7-1) ----------	_____
e. Supervision received	(7-1) ----------	_____
		TOTAL POINTS: _____

III. Risk/Sensitivity Level

High Risk – 6
Moderate Risk – 5
Special-Sensitive – 4

Critical-Sensitive – 3
Noncritical-Sensitive – 2
Low Risk – 1

RISK LEVEL: _____

IV. Final Adjustment Factor(s), *Including AIS Risk Criteria*

Level of Security Clearance Required

☐ TOP SECRET ☐ SECRET ☐ CONFIDENTIAL ☐ NONE

V. Final Risk / Sensitivity Level

Final Risk/Sensitivity Level - _____
Comments:

Level of Investigation Required (To be filled in by the servicing security organization)

☐ NACI ☐ ANACI ☐ MBI ☐ LBI ☐ BI ☐ SSBI

Agency Designator (Type and Print name)	Signature of Agency Designator	Date